スイート B での GET VPN のサポート

スイート B での GET VPN のサポート機能では、Cisco Group Encrypted Transport（GET）VPN に対してスイート B の暗号方式セットのサポートが追加されます。スイート B は、Galois Counter Mode Advanced Encryption Standard（GCM-AES）を含む暗号化アルゴリズムとハッシュ、デジタル署名、キー交換用のアルゴリズムのセットです。

IP Security（IPsec）VPN のスイート B は、RFC 4869、『Suite B Cryptographic Suites for IPsec』でその使用が定義されている標準規格です。スイート B は Cisco IPsec VPN に包括的なセキュリティ拡張機能を提供し、大規模な展開に対して追加のセキュリティを有効にします。スイート B は、リモート サイト間のワイドエリア ネットワーク（WAN）に高度な暗号化セキュリティを必要とする組織に対して推奨されるソリューションです。

スイート B での GET VPN のサポートの前提条件

この機能を有効にするすべてのキー サーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.4 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。この機能は、ネットワークのすべてのデバイスがスイート B をサポートするバージョンであるかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

スイート B での GET VPN のサポートの制約事項

これらが GCM ポリシーまたはガロア メッセージ認証コード（GMAC）トラフィック暗号キー（TEK）ポリシーを使用している場合、グループのすべての連携 KS で同一順序の同一の ACL エントリ（ACE）を持つアクセス コントロール リスト（ACL）を使用する必要があります。そうでない場合、別の KS に登録する GM は、ポリシーのダウンロード後は正しく暗号化および復号化することができません。これは、スイート B では、SPI（TEK に関連付けられているセキュリティ パラメータ インデックス ID）が各 ACL エントリに対して生成され、各 ACL エントリに対して一意であるためです。

既存の ACL のエントリの順序を変更することはできません。したがって、GCM または GMAC TEK ポリシーを使用していて、各 KS に同一順序の同一エントリを持つように各 KS の ACL を更新する必要がある場合は、各セカンダリ KS から ACL を削除し、プライマリ KS で新しい ACL を作成し、セカンダリ KS にそれをコピーしてから、プライマリ KS で **crypto gdoi ks rekey** コマンドを入力して GET VPN ネットワーク全体のキー再生成をトリガーする必要があります。

ip access-list コマンドの **no** 形式（IPv6 を使用している場合は **ipv6 access-list** コマンドの **no** 形式）を使用して ACL を削除します。

Cisco Catalyst 8000 シリーズ エッジ プラットフォームは、GET VPN の Suite B をサポートしていません。Suite B は、次の Cisco ASR 1000 シリーズ アグリゲーション サービス ルータおよび Cisco 4000 シリーズ サービス統合型ルータでのみサポートされています。

表 *1 : GET VEPN Suite B* のサポート

プラットフォーム	モデル	GET VPN Suite B
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	ASR1001-X	対応
	ASR1002-X	対応
	ASR1001-HX	対応
	ASR1002-HX	対応
	ESP100	対応
	ESP200	対応
Cisco 4000 シリーズ サービス統合型ルータ	ISR 4461	対応
	ISR4451-X	対応
	ISR4431	対応

スイート B での GET VPN のサポートに関する情報

スイート B

スイート B は国家安全保障局（NSA）と国立標準技術研究所（NIST）によって標準化されています。スイート B での GET VPN のサポート機能では、これらの暗号化アルゴリズムが GDOI および GET VPN とさまざまな方法（SHA-2/HMAC-SHA-2 と AEC-GCM/AES-GMAC の使用など）で使用できるようにします。

セキュア ハッシュ アルゴリズム 2（SHA-2）は、米国の連邦情報処理標準（FIPS）として NSA により設計され、NIST によって公開された一連の暗号ハッシュ関数（SHA-224、SHA-256、SHA-384、および SHA-512）です。SHA-2 には旧モデル SHA-1 からの多数の変更が含まれます。SHA-2 は 224、256、384、または 512 ビットのダイジェストを含む 4 つのハッシュ関数のセットで構成されます。

HMAC は反復暗号ハッシュ関数を使用するメッセージ認証のメカニズムです。HMAC-SHA-2 は、IPsec の秘密共有キーと組み合わせた SHA-2 バージョン（SHA-224、SHA-256、SHA-384 および SHA-512）反復暗号ハッシュ関数と組み合わせて使用される HMAC です。これらの組み合わせにより、HMAC-SHA-224、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512 と呼ばれます。これらのアルゴリズムは、認証ヘッダー（AH）（ただし GET VPN でサポートされていません）、Encapsulating Security Payload（ESP）、IKE、および IKEv2 プロトコルのデータ発信元の認証および整合性の基礎として、および IKE および IKEv2 の Pseudo-Random Function（PRF）としても使用できます。

GCM を使用する AES（AES-GCM）は、IPsec の暗号化アルゴリズムです。Galois メッセージ認証コードを使用する AES（AES-GMAC）もまた、IPsec に使用されるメッセージの整合性アルゴリズムです。

SHA-2 および HMAC-SHA-2

スイート B での GET VPN のサポート機能では、ハッシュおよび署名アルゴリズムとして SHA-2 および HMAC-SHA-2（HMAC-SHA-256、384、および 512）を使用することができます。256、384、および 512 ビット キーによる SHA-2 および HMAC-SHA-2 は次に使用されます。

- RFC 6407、『The Group Domain of Interpretation』の セクション 3.2（KS と GM 間の認証）で説明されているハッシュアルゴリズムとして IKEv1 を使用する GDOI 登録。
- KS からのキー再生成メッセージの認証および GM からの確認応答メッセージの認証のためのキー再生成メッセージをハッシュ化する Key Encryption Key（KEK）キー再生成ポリシー。
- IPsec SA 整合性チェックのための HMAC-SHA-2 の TEK IPsec ポリシー。

AES-GCM と AEC-GMAC

256、384、および 512 ビット キーによる AES-GCM（AES-GCM-128、192、および 256）および AES-GMAC（AES-GMAC-128、192、および 256）暗号化アルゴリズムは、IPsec SA 暗号化および整合性アルゴリズムとして TEK IPsec ポリシーで使用されます。GCM は暗号化および整合性に使用され、GMAC は整合性のみに使用されます。

スイート B に準拠する暗号化アルゴリズムのセット

RFC 4869 には IKE および IPsec を使用する 4 セットの暗号化アルゴリズムが定義されています。設定すると、これらのいずれかのセットがスイート B に準拠します。各セットは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー アグリーメント アルゴリズム、およびハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されます。

- Suite-B-GCM-128：128 ビット AES-GCM を使用して ESP の整合性の保護と機密性を提供します（RFC 4106、『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』を参照してください）。ESP の整合性の保護および暗号化が両方必要な場合はこのスイートまたは Suite-B-GCM-256 を使用します。
- Suite-B-GCM-256：256 ビット AES-GCM を使用して ESP の整合性の保護と機密性を提供します（RFC 4106、『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』を参照してください）。ESP の整合性の保護および暗号化が両方必要な場合はこのスイートまたは Suite-B-GCM-128 を使用します。
- Suite-B-GMAC-128：128 ビット AES-GMAC を使用して ESP の整合性の保護を提供します（RFC 4543、『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』を参照してください）が、機密性は提供しません。ESP 暗号化の必要がない場合にのみこのスイートまたは Suite-B-GMAC-256 を使用します。
- Suite-B-GMAC-256：256 ビット AES-GMAC を使用して ESP の整合性の保護を提供します（RFC 4543、『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』を参照してください）が、機密性は提供しません。ESP 暗号化の必要がない場合にのみこのスイートまたは Suite-B-GMAC-128 を使用します。

シスコのソフトウェアでは、これらのどのアルゴリズムも設定できます。スイート B での GET VPN のサポート機能では、GET VPN でこれらのアルゴリズムを使用できます。

SID 管理

GET VPN のカウンタ ベースの動作モード（ESP-GCM-AES など）では、初期化ベクトル（IV）をグループ キーで再利用しない必要があります。そのため、この機能では KS が IV 作成のための一意の送信者 ID（SID）を各 GM（インターフェイスごと）に割り当てることができる方法が提供されています。

スイート B の IPsec SA 暗号化および整合性アルゴリズムとして使用される TEK IPsec ポリシーには、GM にこれらの一意の SID 値（GMSID）を配布するため、KS で一意の SID 値のプールの管理が必要です。それぞれの連携 KS には割り当てる GMSID の個別のプールが必要です。各 KS はこれらの SID プールを設定するために一意の KS SID（KSSID）を設定します。

SID の領域は、KSSID 部と GMSID 部の 2 部に分けられます。したがって、SID は KSSID と GMSID の連結であり、KSSID は SID の KS 部、GMSID は SID の GM 部です。SID は次のビットによって形成されます。

```
 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                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

この例では、各 KSSID（0 ～ 127）に 2^{17}（131,072）の GMSID があり、登録する各 GM に動的に割り当てられます。

GM は GMSID を使用して、AES-GCM または AES-GMAC を使用するときに指定したキーで送信される各パケットに対して一意の 64 ビット IV を形成します。IV は次のバイトで形成されます。

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

送信者固有の IV（SSIV）は、パケット カウンタです。

グループ サイズ

グループ サイズは、GM への配布のため KS に予約されている KSSID および GMSID の SID スペース割り当ての長さです。使用可能なグループサイズには、小（8、12、または16ビット）、中（24 ビット、デフォルト）、大（32 ビット）があります。中は、ほぼすべてのネットワークに適しています。

大のグループサイズは、マニュアル『 Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program 』のセクション A.5 「Key/IV Pair Uniqueness Requirements from SP 800-38D」の要件（Suite B と組み合わせて使用される GET VPN に 2^{32} 以上の使用可能な固有の「モジュール名」（SID）がある必要がある）に厳密に準拠する必要がある場合にのみ使用する必要があります。このマニュアルは、NIST および Communications Security Establishment Canada（CSEC）によって発行および管理されています。

たとえば、KS 1 台の大のグループ サイズで SID は 32 ビットであり、512 個の KSSID 値（0 ～ 511 の範囲）があり、それぞれに GM の登録に配布する GMSID が 8,388,607 個あります。大のグループ サイズでは、次の KSSID 割り当てのガイドラインを使用して、KSSID の範囲を設定します。

表 *2 :* グループ サイズ大に推奨される *KSSID* 範囲

KS	1 台の KS（連携 KS なし）	2 台の連携 KS	3 台の連携 KS	4 台の連携 KS
KS1	0 - 511	0 - 255	0 - 127	0 - 63
KS2	—	256 - 511	128 - 255	64 - 127

KS	1 台の KS（連携 KS なし）	2 台の連携 KS	3 台の連携 KS	4 台の連携 KS
KS3	—	—	256 - 383	128 - 191
KS4	—	—	384 - 511	192 - 255
KS5	—	—	—	256 - 319
KS6	—	—	—	320 - 383
KS7	—	—	—	384 - 447
KS8	—	—	—	448 - 511

最初に元の KS を設定し、より多くの KS を含めるように連携 KS ネットワークを拡張する予定の場合、上の表の列にはネットワークで予想される KS の数を使用し、後で新しい KS を追加できるようにします。

小（8、12、または 16 ビット）のグループサイズは、RFC 6054、『Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic』に従って、8、12、および16 ビットの SID 長さで厳格な相互運用性が要求される、よく理解されている状況でのみ使用する必要があります。このような相互運用性が必要な場合、グループごとの SID の数が厳しく制限される（これにより KS および GM の数が厳しく制限される）ため、ネットワークの設計時は注意が必要です。小グループ サイズの制限を次に示します。

表 *3:* グループ サイズ小の制限

SID 長さ	KSSID（合計 KS）	KSSID ごとの GMSID	GMSID（合計 GM）	KS 1 台に可能な GM 登録数（すべての KS に KSSID を均等に割り当てた後）			
—	—	—	—	1 KS	2 KS	4 KS	8 KS
8 ビット	2	128	255	320	96	—	—
12 ビット	4	1,024	4,095	3,840	1,792	768	—
16 ビット	16	4,096	65,535	64,512	31,744	15,360	7,168

連携キー サーバへの KSSID 割り当て

設定されたグループ サイズ、KS の数、GM の数、KS ごとの GM の数、および KS または GM（または両方）の将来の拡張に基づいて、最初の GDOI KS ID（KSSID）の数を各 KS に割り当てるよう前もって計画する必要があります。

GDOI グループに複数の連携 KS があるときは、各 KS が固有の KSSID 値のセットを持つようにして、登録する GM が、グループ内の登録する別の GM と同じ SID を受け取らないようにする必要があります。このため、連携 KS の数と、連携 KS を後で追加するかどうかを考慮しつつ、連携 KS 全体に KSSID をどのように割り当てるのかを前もって計画する必要がありま

す。何も追加しない場合、すべての KS で利用可能なすべての KSSID を割り当てることができます。連携 KS を追加する場合、一部の KSSID を予約し、それらの KS をネットワークに追加するときに割り当てる必要があります。

KSSID は再割り当てできます。ただし、GMSID を配布するために KS によってすでに使用されている KSSID を KS から削除する場合、グループはトラフィックを損失することなく再初期化されます（つまり、すべての GM が強制的に再登録を行い、TEK IPsec SA のキー再生成が行われて使用済みの KSSID がリセットされます）。このグループの再初期化を回避するには、（中のデフォルト グループ サイズを使用する）次の表のガイドラインを使用します。

表 *4*：連携 *KS*（グループ サイズ中）の推奨される *KSSID* 割り当て範囲

	1 台の KS（連携 KS なし）	**2 台の連携 KS**	**3 台の連携 KS**	**4 台の連携 KS**
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

より多くの KS を含めるように連携 KS ネットワークを拡張する予定の場合、最初に元の KS を設定するときは、上の表の列には拡張したネットワークで予定される KS の数を使用し、後で新しい KS を追加できるようにします。

次に、KS に KSSID を割り当てるための追加のガイドラインを示します。

- KS 全体の KSSID の連続するブロックのみを設定します（例：KS1 = 0-9 + 40-49、KS2 = 10-19 + 50-59、KS3 = 20-29、KS4 = 30-39 など）。
- 任意の 1 台の KS には、（他の KS が GM 登録をすべて失敗した場合）グループからすべての GM 登録を受信するために十分な KSSID のスペースがある必要があります。
- グループの再初期化を回避するには、新しい KSSID の値または範囲だけを追加します。必要な場合を除き、これらは削除しないでください。
- ネットワーク分割（連携 KS 間の接続の損失）の間は、KSSID の割り当てを変更しないでください。これにより、マージ時（連携 KS 間の接続の回復時）に再初期化を引き起こす可能性がある KSSID の重複を防ぎます。
- グループが *n* とおりの分割（セカンダリ KS が計画されるがまだ設定されていないという意味）を開始する場合は、すべての KSSID をグループが分割されていないかのように設定します。

使用可能な KSSID の数は、次の表のように、グループ サイズの設定に依存します。

表 *5:* グループ サイズに基づく使用可能な *KSSID* の範囲

設定されたグループサイズ	使用可能な KSSID の数
小（8 ビット）	0 ～ 1
小（12 ビット）	0 ～ 3
小（16 ビット）	0 ～ 15
中	0 ～ 127
大	0 ～ 511

グループの再初期化

グループの再初期化は、KSSID を廃棄するプロセスです。グループの再初期化は、すべての KS にわたって発生します（プライマリおよびセカンダリ）。どの KS もグループの再初期化をトリガーでき、次のときに発生します。

- 非 GCM から GCM に TEK ポリシーを変更する。
- グループ サイズを変更する。
- 以前に使用した KSSID を削除する。
- グループの KS が KSSID と GMSID の両方を使い果たした。
- 連携 KS によって検出された KSSID の重複が解決された。

再初期化では、すべての KS が使用済みの KSSID を古い（使用済みの）KSSID に移動します（それにより廃棄されます）。次に、再初期化によって新しい KEK と新しい TEK が作成され、既存の TEK ライフタイムが短くなり、既存の TEK が削除され、すべての GM が再登録します（**clear crypto gdoi ks members** コマンドによって決定される期間内）。この期間は残りのライフタイムの 5 % であり、90 秒から 1 時間の間です。既存の TEK のライフタイムが期限切れになると、各 KS は古い（使用済み）KSSID をリセットするため、すべての KSSID が再度使用可能になります。

再初期化により GM でトラフィックが中断されることはありません。すべての GM は登録時に新しい TEK を含む新しい GMSID を受信します。

スイート B の Cisco GET VPN システム ロギング メッセージ

次の表では、スイート B に関連する GET VPN システム ロギング（syslog とも呼ばれます）メッセージについて説明します。

表 *6 : KS* および連携 *KS* メッセージ

メッセージ	説明
%GDOI-5-KS_REINIT_GROUP: *reason* for group *group-name* and will re-initialize the group.	KS はグループを再初期化します。表示される可能性のある *reason* の文字列は、次のとおりです。 • 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.	グループの再初期化が完了しました。一部の操作は再初期化中（グループ サイズの変更時や使用する KSSID の削除時など）にブロックされるため、再初期化がいつ完了したのかを確認するのに役立ちます。再初期化は、古い（使用した）TEK がクリアされるまで終了しません。これは、再初期化が再度チェックされるか（**show** コマンドの実行時、グループ サイズまたは KSSID の設定時、または連携 KS の更新時など）、次の GM が登録するまで発生しないことがあります。
%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.	（GCM の使用時と GM が登録を開始した後）グループの GM は SID を必要としますが、KS に設定された KSSID がないか、それ以上使用可能な SID がありません。

メッセージ	説明
%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).	別のグループの連携 KS ピアと重複する KSSID または KSSID 範囲が GM 登録をブロックしています。重複する KSSID 設定は CLI によって連携 KS でブロックされますが、GET VPN ネットワークの分割シナリオ（1 つ以上の連携 KS が一時的に使用できなかったがオンラインに戻った場合）や保存済みの設定を使用するとこれが生じることがあります。
%GDOI-5-COOP_KS_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID) with COOP-KS peer allowing GM registrations once again.	連携 KS ピアと重複する KSSID が解決されました（GM 登録を再開できます）。

表 *7: GM* メッセージ

メッセージ	説明
%GDOI-5-GM_IV_EXHAUSTED: GM for group *group-name* exhausted its IV space for interface *interface-name* and will re-register.	グループの GM が特定の SA の IV スペース（固有の IV のセットの意味）を使い尽くしたため、再登録します。
%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.	クライアントのキー再生成ハッシュ アルゴリズム（指定された KEK ポリシー）が指定されたグループの GM によって承認されませんでした。登録時に GM が KEK ポリシーを拒否しました。
%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.	データ保護のクライアントのキー再生成トランスフォーム セット（指定された TEK ポリシー）が GM によって承認されませんでした。登録時に GM が TEK ポリシーを拒否しました。
%GDOI-5-GM_REKEY_TRANSFORMSET_CHECK_FAIL: The transform set (*transform-set*) for data protection in group *group-name* is unacceptable by this client.	グループのデータ保護のトランスフォーム セットがクライアントによって承認されませんでした。GM がキー再生成を受け取り、TEK ポリシーを拒否しました。

メッセージ	説明
%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.	RSA キーのモジュラス長が十分にないため、キー再生成のシグニチャ ハッシュ アルゴリズムの設定が拒否されました。HMAC-SHA-384 は少なくとも 465 ビット（バイトの 59 ブロック）のモジュラスを必要とし、HMAC-SHA-512 は 593 ビット（バイトの 75 ブロック）のモジュラスを必要とします。

スイート B での GET VPN のサポートの設定方法

スイート B での GET VPN のサポート機能セットの各機能は個別に設定可能です。しかし、スイート B の標準に準拠するため、特定の組み合わせでこれらの機能を設定する必要があります。これらの組み合わせの詳細については、RFC 4869、『 Suite B Cryptographic Suites for IPsec 』を参照してください。

GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する

GET VPN はグループに基づいた技術であるため、（プライマリ KS、連携 KS、および GM を含めた）同じグループ内のすべてのデバイスは、機能を有効化するためにスイート B の機能をサポートする必要があります。グループの機能を有効にするには、グループ内のすべてのデバイスが GET VPN ソフトウェアの互換性のあるバージョンを実行していることを確認する必要があります。

GET VPN ネットワークのすべてのデバイスがスイート B をサポートしていることを確認するには、KS（またはプライマリ KS）で次のステップを実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**show crypto gdoi feature suite-b** 例： `Device# show crypto gdoi feature suite-b`	ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスがスイート B をサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature suite-b | include No** 例： `Device# show crypto gdoi feature suite-b | include No`	（オプション）スイート B をサポートしないデバイスのみ検索します。

GET VPN スイート B でのキー サーバの設定

KEK の署名ハッシュ アルゴリズムの設定

KEK の署名ハッシュ アルゴリズムを設定するにはこの作業を行います。

始める前に

この作業には次の前提条件があります。

- デバイスに関連付けられている RSA キー ペアを使用するキー再生成認証が有効になっていることを確認します。これを行うには、**rekey authentication** コマンドを **mypubkey rsa** *key-name* キーワードと引数で使用します。
- RSA キー ペアに十分な長さのモジュラスがあることを確認します。HMAC-SHA-384 は少なくとも 465 ビット（バイトの 59 ブロック）のモジュラスを必要とし、HMAC-SHA-512 は 593 ビット（バイトの 75 ブロック）のモジュラスを必要とします。キー再生成の署名ハッシュ アルゴリズムが不十分なモジュラス長のキー ペアを使用する SHA-384 または SHA-512 に変更されると、設定拒否メッセージがコンソールに表示され、システム ログ メッセージが生成されます。同様に、キー再生成の署名ハッシュ アルゴリズムがすでに SHA-384 または SHA-512 であり、キーペアが不十分なモジュラス長の 1 つに変更されると、同様のメッセージがコンソールに表示され、同じシステム ログ メッセージが生成されます。
- キー再生成メッセージを受信した後の GM から KS への確認応答の認証に SHA-2/HMAC-SHA-2 を使用するには、GM へのキー再生成メッセージのユニキャスト配信を有効にする必要があります。これを実行するには、**rekey transport unicast** コマンドを使用します。

手順の概要

1. **enable**

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**rekey sig-hash algorithm** *algorithm* 例： `Device(gdoi-local-server)# rekey sig-hash algorithm sha512`	KEK の署名ハッシュ アルゴリズムを設定します。Suite B の場合は、**sha256**、**sha384**、または **sha512** を指定する必要があります。
ステップ 6	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ サイズの設定

このタスクはオプションです。ほぼすべての展開で、メディアのデフォルト グループ サイズ（送信者識別子の長さ）が推奨されます。スイート B のグループ サイズを設定するにはこの作業を行います。

スイート B（つまり ESP-GCM または ESP-GMAC）が設定され、スイート B のポリシーが生成された後で、連携 KS を使用するグループのグループ サイズを変更する場合、プライマリ KS で変更する前にすべてのセカンダリ KS でグループ サイズを変更する必要があります。

グループ サイズを変更すると（新しい SID 長が使用できるように）グループが初期化されます。KS 全体で競合するグループ サイズ設定があると GM 登録がブロックされます。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group size** {**small** {**8** | **12** | **16**} | **medium** | **large**} 例： `Device(gdoi-local-server)# group size small 16`	グループ サイズを設定します。
ステップ 6	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

キー サーバ識別子の設定

スイート B では、それぞれの GM に固有の GMSID の割り当てが必要です。これは GM が以前同じキーに（その GM または別の GM が）使用した SID を再利用できないことを意味します。したがって、GET VPN が重複する SID 値を許可しないように設計されていても、KS ごとに固有のセットを持つように KS 間の KSSID 値を正しく設定する必要があります。（KS 間の KSSID が重複すると再初期化されます。）

KS に SID のプールを割り当てるには少なくとも 1 つの KSSID を設定する必要があります。TEK IPSec ポリシーとして GCM または GMAC を設定する前に KS でこれを行います。

この作業を行って KS に KSSID または KSSID の範囲を割り当てます。各 KS は、GCM または GMAC を使用する際には少なくとも 1 つの KSSID を割り当てる必要があります。単一の KSSID、KSSID の範囲、またはその両方を設定できます。メディアのデフォルト グループ サイズとして、0 ～ 127 の範囲の 128 個の利用可能な KSSID 値があります。

KSSID 値は、GDOI ローカル サーバ ID コンフィギュレーション モードを終了するまで KS に割り当てられません（KS から使用もできません）。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**identifier** 例： `Device(gdoi-local-server)# identifier`	GDOI ローカル サーバ ID コンフィギュレーション モードを開始します。
ステップ 6	**range** *lowest-kssid - highest-kssid* 例： `Device(gdoi-local-server-id)# range 10 - 20`	KSSID の範囲を割り当てます。 • この範囲は、グループ全体で一意である必要があります。
ステップ 7	**value** *kssid* 例： `Device(gdoi-local-server-id)# value 0`	KSSID を割り当てます。 • この KSSID は、グループ全体で一意である必要があります。 • **value 0** コマンドは、KSSID 値 0 で始まる SID のプールを KS に割り当てます（つまり 0x0 で始まり 0x1FFFF で終わる SID 値のプールが割り当てられます）。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(gdoi-local-server-id)# end`	GDOI ローカル サーバ ID コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

すでに別の KSSID が割り当てられている KS に 1 つ以上の KS を設定しようとすると（かつ連携 KS ネットワークが分割されていないと）、設定は拒否され、GDOI ローカル サーバ ID コンフィギュレーション モードを終了すると次のメッセージが表示されます。

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

連携 KS ネットワークが分割されている場合、重複する KSSID を設定する必要はありません。ネットワークのマージで KSSID の重複が検出されると、GM の登録は重複が解決するまでブロックされます。次のシステム ログ メッセージが両方の KS に表示されます。

```
%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)
```

KS が重複する KSSID を構成解除すると、グループはトラフィックを損失することなく再初期化します（つまり、すべての GM が再登録を強制され、TEK IPSec SA は使用された KSSID をリセットするためにキー再生成されます）。次のシステム ログ メッセージが KS に表示されます。

```
%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.
```

%GDOI-5-KS_SEND_UNICAST_REKEY システム ログ メッセージは、これがプライマリ KS である場合にのみ表示されます。KSSID が重複しているピア KS でも %GDOI-5-COOP_KSSID_OVERLAP_RESOLVED システム ログ メッセージが表示されます。

スイート B の IPsec SA の設定

スイート B の IPsec SA を設定するには、次のステップを実行します。

手順の概要

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. 次のいずれかのコマンドを入力します。
   - **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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**] 例： `Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	トランスフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • スイート B では、ESP-GCM または ESP-GMAC を使用するトランスフォーム セットを指定する必要があります。（別のコマンドラインにコマンドをもう一度入力して、複数のトランスフォーム セットを定義できます。） • オプションで 128、192、または 256 のキー サイズを指定できます。デフォルトのキーのサイズは 128 です。
ステップ 4	**crypto ipsec profile** *ipsec-profile-name* 例： `Device(config)# crypto ipsec profile profile1`	IPsec プロファイル（2 つの IPsec ルータ間の IPsec 暗号化に使用されるパラメータ）を定義して、IPsec プロファイル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**set transform-set** *transform-set-name* 例： `Device(ipsec-profile)# set transform-set transformset1`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 6	**exit** 例： `Device(ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーション モードを終了します。
ステップ 7	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。

ステップ 8	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。
		• **identity number** *number* コマンドは IPv4 および IPv6 の構成に適用されます。
		• **identity address ipv4** *address* コマンドは、IPv4 構成のみに適用されます。

ステップ 9	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 10	**sa ipsec** *sequence-number* 例： `Device(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 11	**profile** *ipsec-profile-name* 例： `Device(gdoi-sa-ipsec)# profile gdoi-p`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 12	**match address** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*} 例：	GDOI 登録の IP 拡張アクセス リスト（ACL）を選択します。

	コマンドまたはアクション	目的

	`Device(gdoi-sa-ipsec)# match address ipv4 102`	• IPv4 グループに対しては **ipv4** キーワード、IPv6 グループに対しては **ipv6** キーワードを使用する必要があります。
		• IPv6 構成には（番号付きではなく）名前付きアクセス リストを使用する必要があります。
		（注） 必ずグループのすべての連携 KS の中で同一順序で同一エントリを持つ ACL を選択してください。そうでない場合、別の KS に登録する GM は、ポリシーのダウンロード後は正しく暗号化および復号化することができません。
		（注） IPv6 グループに IPv4 のポリシーを割り当てようとするると、アクセス リスト名が無効であるか、リストはすでに存在するが誤った種類であることを示すエラー メッセージが表示されます。
		`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.`

ステップ 13	**end** 例： `Device(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN スイート B でのグループ メンバーの設定

スイート B の KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

GM によって許可される KEK 用の スイート B 暗号化およびハッシュ アルゴリズムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. 次のいずれかのコマンドを入力します。

- **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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例： `Device(config-gdoi-group)# server address ipv4 10.0.5.2`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**client rekey encryption** *cipher* [... [*cipher*]] 例：	KEK のクライアント受け入れ可能キー再生成暗号化を設定します。

	コマンドまたはアクション	目的
	`Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256`	
ステップ 7	**client rekey hash** *hash* 例： `Device(config-gdoi-group)# client rekey hash sha384`	KEK のクライアント受け入れ可能ハッシュを設定します。 • Suite B の場合は、**sha256**、**sha384**、または **sha512** のいずれかを指定する必要があります。
ステップ 8	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイート B の TEK の受け入れ可能トランスフォーム セットの設定

GM によって許可されるデータ暗号化または認証のために TEK が使用するトランスフォーム セットを設定するには、次のステップを実行します。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name* {**esp-gcm**	**esp-gmac**} [**128**	**192**	**256**] 例：	トランスフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）

	コマンドまたはアクション	目的
	`Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • スイート B では、ESP-GCM または ESP-GMAC を使用するトランスフォームセットを指定する必要があります。 • 別のコマンドラインにコマンドをもう一度入力して、複数のトランスフォームセットを定義できます。 • オプションで 128、192、または 256 のキー サイズを指定できます。デフォルトのキーのサイズは 128 です。
ステップ 4	**exit** 例： `Device(cfg-crypto-trans)# exit`	暗号化トランスフォーム コンフィギュレーション モードを終了します。
ステップ 5	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 6	**client transform-sets** *transform-set-name1* [*...* [*transform-set-name6*]] 例： `Device(config-gdoi-group)# client transform-sets g1`	データの暗号化および認証のために TEK によって使用される受け入れ可能トランスフォームセット タグを指定します。 • トランスフォーム セット タグは 6 個まで指定できます。
ステップ 7	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイート B での GET VPN のサポートの確認とトラブルシューティング

キー サーバ上のスイート B での GET VPN のサポートの確認とトラブルシューティング

KS で実行されている設定を表示するには、**show running-config** コマンドを使用します。

手順の概要

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**

手順の詳細

ステップ 1 **show crypto gdoi ks identifier** [**detail**]

例：

```
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
```

このコマンドは、スイート B の SID 管理の状態を表示します。Transform Mode フィールドは SID 管理およびスイート B のポリシーがグループ内で現在使用されているかどうかを確認するために非カウンタ（非スイート B）またはカウンタ（スイート B）のいずれかにできます。グループが現在再初期化（つまり、すべての GM が再登録を強制され、TEK IPsec SA がキー再生成されて使用済みの KSSID をリセットする）を行っている場合は、reinitializing フィールドに Yes が表示されます。SID Length (Group Size) フィールドは、グループで現在使用されているグループ サイズを決定します。デフォルトは 24 ビット（中）です。

Current KSSID In-Use フィールドおよび Last GMSID Used フィールドは、次の登録 GM に分配される SID（または SIDS）に対応します。KSSID (or SIDS) Assigned フィールドは、連携 KS と同期した、ローカルに設定されている KSSID に対応します。Available KSSID (or SIDS) フィールドは、最後の再初期化以降まだ使用されていない KSSID に対応します。新しい KSSID を使用するたびに KSSID (or SIDS) Used フィールドに追加され、再初期化時に、これらの使用された KSSID が KSSID (or SIDS) Used (Old) フィールドに移動されます。再初期化期間の終わりに、古い使用済みの KSSID がクリアされて再び Available KSSID プールに加えられます。

（注） # of SIDs Remaining until Re-init フィールドの値が 0 に近づくと、GM が再登録を継続している場合はすぐに再初期化が発生します。再初期化によってトラフィックの中断やネットワークの問題が発生することはありませんが、すべての GM がの再登録が発生します。

ステップ 2 **show crypto gdoi ks coop identifier** [**detail**]

例：

```
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
```

このコマンドは、連携 KS 全体で同期化された SID のステータス情報を表示します。

KSSID Overlap フィールドに Yes が表示されると、KSSID の重複（ネットワークの分割時に発生することがあります）が解決するまで GM 登録がブロックされます。GM 登録を再開するには、1 つの連携 KS またはほかの KS から重複している KSSID を構成解除する必要があります。重複する KSSID が解決すると、再初期化が発生します。

グループ サイズを変更すると（ほとんどの導入では推奨されません）、すべてのセカンダリ KS で最初に新しいグループ サイズを設定する必要があります。次にプライマリ KS で、SID Length (Group Size) Cfg フィールドに、すべての連携 KS ピアの新しいグループ サイズが表示されます。プライマリ KS で新しいグループ サイズを設定したときのみ、すべての KS が新しいグループ サイズの使用を開始し、SID Length (Group Size) Used フィールドを更新して新しいグループ サイズを表示します。

ステップ 3 **show crypto gdoi feature suite-b**

例：

```
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
```

このコマンドは、KS および GM がスイート B 機能セット（つまり、AES-GCM、AES-GMAC、SHA-2、および HMAC-SHA2）を使用できるかどうかを表示します。Version フィールドが 1.0.4 またはそれ以上を表示し、Feature Supported フィールドが連携 KS グループ内のすべての KS、および登録されている GM について Yes を表示する必要があります。

ステップ 4 show crypto gdoi ks policy

例：

```
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
```

このコマンドは、TEK および IPSec SA が ESP-GCM または ESP-GMAC の TEK ポリシーの access-list フィールド内の ACL から（Selector フィールドに表示される）ACE ごとに生成されているかどうかを表示します。またこのコマンドは、KEK ポリシーが署名ハッシュ アルゴリズムとして SHA-2/HMAC-SHA-2 を使用しているかどうかも表示します。

GM 上のスイート B での GET VPN のサポートの確認とトラブルシューティング

GM で実行されている設定を表示するには、**show running-config** コマンドを使用します。

手順の概要

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

手順の詳細

ステップ 1 **show crypto gdoi gm identifier** [**detail**]

例：

```
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)
```

このコマンドは、GM が GCM-AES または GMAC-AES を TEK IPsec SA ポリシーとして使用しているときに受信してインストールされた SID のステータスを表示します。Transform Mode フィールドでは、SID がダウンロードされ、インストールされているかどうか、およびスイート B のポリシーがグループで使用されているかどうかを確認するために、非カウンタ（非スイート B）またはカウンタ（スイート B）を表示できます。# of SIDs Last Requested フィールドは、主にこの登録されている（つまり、ローカル アドレスまたはクライアント登録インターフェイスを使用している）GM のために暗号マップが適用されるインターフェイスの数に依存します。SID は、ローカル アドレスを使用している場合は Shared Across Interfaces フィールドであり、各 CM の Installed SID Range フィールドも同じになります。このコマンドは、主に各 CM インターフェイスにインストールされている SID があることを確認するために使用します。

ステップ 2 show crypto gdoi feature suite-b

例：

```
Device# show crypto gdoi feature Suite B

       Version    Feature Supported
        1.0.4           Yes
```

このコマンドは、この GM がスイート B 機能セット（つまり、GCM-AES、GMAC-AES、SHA-2、および HMAC-SHA-2）を使用できるかどうかを表示します。Version フィールドが 1.0.4 またはそれ以上を表示し、Feature Supported フィールドが Yes を表示する必要があります。

ステップ 3 show crypto gdoi

例：

```
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
```

複数の IPsec SA のプレゼンスは、GCM または GMAC が設定されていることを示します（各 IPSec SA にはダウンロードした各 ACE の固有の SPI があることに注意してください）。TEK POLICY for the current KS-Policy ACEs Downloaded セクションの TEK POLICY に記載されている各 ACE に関して、このコマンドは、TEK ポリシーおよび IPsec SA が ACL Downloaded From KS に記載されている ACL からダウンロード（およびインストール）されているかどうかを表示します。またこのコマンドは、KEK ポリシーが署名ハッシュ アルゴリズム（たとえば、HMAC_AUTH_SHA256）に SHA-2/HMAC-SHA-2 を使用しているかどうかも表示します。

スイート B での GET VPN のサポートの設定例

例：GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスがスイート B 暗号化をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
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
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）でスイート B をサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
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
```

例：GET VPN スイート B のキー サーバの設定

KEK の署名ハッシュ アルゴリズムの設定

次に、KEK の署名ハッシュ アルゴリズムを設定する方法の例を示します。

```
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
```

スイート B のグループ サイズの設定

メディアのデフォルトのグループ サイズはほとんどの導入に十分であるため、スイート B のグループ サイズの設定はオプションです。次の例は、スイート B にグループ サイズを設定する方法を示しています。

```
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
```

キー サーバ識別子の設定

次の例では、KS に KSSID および KSSID の範囲を割り当てる方法を示します。

```
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
```

スイート B の IPsec SA の設定

次の例では、スイート B の IPsec SA を設定する方法を示します。この例では、アイデンティティ アドレスではなくアイデンティティ番号を使用します。

```
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
```

例：GET VPN スイート B のグループ メンバーの設定

スイート B の KEK の暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

次の例は、GM によって許可される KEK のスイート B 暗号化およびハッシュ アルゴリズムの設定方法について説明します。この例では、アイデンティティ アドレスを使用します（IPv4データ プレーン構成とのみ互換性）。代わりにアイデンティティ番号を使用できます（IPv4 および IPv6 データ プレーン構成と互換性）。

```
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
```

スイート B の TEK の受け入れ可能トランスフォーム セットの設定

次の例は、データ暗号化または認証のために TEK が使用する受け入れ可能トランスフォーム セットを設定する方法を示します。

```
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
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
IKE および IKE ポリシーの設定作業 IPsec トランスフォームの設定作業	『Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2M&T』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール

関連項目	マニュアル タイトル
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』

標準および RFC

標準/RFC	タイトル
連邦情報処理標準（FIPS）パブリケーション 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』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

スイート B での GET VPN のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8 :* スイート *B* での *GET VPN* のサポートの機能情報

機能名	リリース	機能情報
スイート B での GET VPN のサポート		スイート B での GET VPN のサポート機能では、Cisco Group Encrypted Transport（GET）VPN に対してスイート B の暗号方式セットのサポートが追加されます。スイート B は、Galois Counter Mode Advanced Encryption Standard（GCM-AES）を含む暗号化アルゴリズムとハッシュ、デジタル署名、キー交換用のアルゴリズムのセットです。IP Security（IPsec）VPN 用のスイート B は、RFC 4869 で使用法が定義されている標準です。スイート B は Cisco IPsec VPN に包括的なセキュリティ拡張機能を提供し、大規模な展開に対して追加のセキュリティを有効にします。スイート B は、リモート サイト間のワイドエリア ネットワーク（WAN）に高度な暗号化セキュリティを必要とする組織に対して推奨されるソリューションです。 次のコマンドが導入または変更されました。 **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.**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。