CHAPTER 27

IPSec VPN SPA を使用した IKE 機能の設定

この章では、Cisco 7600 シリーズ ルータ上の IPSec VPN SPA を使用して Internet Key Exchange（IKE; インターネット キー エクスチェンジ）関連機能を設定する方法について説明します。具体的な内容は次のとおりです。

（注） Internet Key Exchange（IKE）に関する詳細は、次の Cisco IOS マニュアルを参照してください。

次の URL の『*Cisco IOS Security Configuration Guide*』*Release 12.2*
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

次の URL の『*Cisco IOS Security Command Reference*』*Release 12.2*
http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

システム イメージおよびコンフィギュレーション ファイルの管理については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』および『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章で使用するコマンドの詳細については、『*Cisco IOS Software Releases 12.2SR Command References*』および『*Cisco IOS Software Releases 12.2SX Command References*』を参照してください。また、関連する CiscoIOS Release12.2 ソフトウェア コマンド リファレンスおよびマスター インデックスも参照してください。詳細については、「関連資料」（P.1i）を参照してください。

ヒント IPSec VPN SPA を使用して VPN を正しく設定するために、設定の概要および注意事項にすべて目を通してから設定作業を始めてください。

IKE の概要

IKE は、IPSec 標準と組み合わせて使用されるキー管理プロトコル標準です。IKE を使用しなくても IPSec を設定できますが、IKE を使用すると IPSec 標準に機能が追加され、柔軟性が高まり、設定が容易になって、IPSec が強化されます。

（注）　IKE の詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

IKE は自動的に IPSec SA（セキュリティ アソシエーション）とネゴシエーションし、負担のかかる手動での事前設定を行わなくても、IPSec セキュア通信を実行できるようになります。IKE には特に次の利点があります。

- 両方のピアの暗号マップで、すべての IPSec セキュリティ パラメータを手動で指定する必要がなくなります。

（注）　Cisco IOS Release 12.2SRA 以降、手動キー入力はサポートされなくなりました。

- IPSec SA のライフタイムを指定できます。
- IPSec セッション中に、暗号キーを変更できます。
- IPsec でアンチリプレイ サービスを実行できます。
- 管理可能でスケーラブルな IPSec を実装するために、CA（認証局）サポートが許可されます。
- ピアのダイナミック認証が可能になります。

IKE ネゴシエーションは保護する必要があるため、共通の（共有された）IKE ポリシーについて両方のピアが合意することにより、各 IKE ネゴシエーションは開始します。このポリシーでは、以降の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを記述し、ピアの認証方法を規定します。ユーザは IKE ネゴシエーションに関与するピアごとに、IKE ポリシーを作成する必要があります。

IKE ポリシーを設定しない場合は、デフォルト ポリシー（常に最小プライオリティに設定され、各パラメータのデフォルト値を格納しているポリシー）が使用されます。

2 つのピアがポリシーについて合意すると、各ピアで確立された SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーション中にこれらの SA が以降のすべての IKE トラフィックに適用されます。

各ピアに、プライオリティが設定された複数のポリシー（それぞれパラメータ値の組み合わせが異なる）を設定できます。ただし、これらのポリシーの少なくとも 1 つに、リモート ピアのポリシーの 1 つとまったく同じ暗号、ハッシュ、認証、および Diffie-Hellman パラメータ値を格納する必要があります。作成したポリシーごとに、一意のプライオリティを割り当てます（1 ～ 10,000 で、1 が最大プライオリティ）。

IKE ポリシー マップでの AES の設定

Advanced Encryption Standard（AES; 高度暗号化規格）は、Data Encryption Standard（DES; データ暗号規格）の後継として開発された IPSec および IKE のプライバシー トランスフォームです。AES は DES よりも安全度の高い設計となっています。AES ではキーのサイズが従来より大きく、侵入者がメッセージを解読するには、あらゆるキーを試してみるしか方法がありません。AES ではキーの長さは可変であり、128 ビット（デフォルト）、192 ビット、または 256 ビットのキーを指定できます。

IKE ポリシー マップ内で AES 暗号化アルゴリズムを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto isakmp policy priority`	ISAKMP ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。 • *priority* : IKE ポリシーを指定し、このポリシーにプライオリティを割り当てます。1 ～ 10,000 の整数を使用します。プライオリティは 1 が最高、10,000 が最低です。
ステップ 2	`Router(config-isakmp)# encryption {aes | aes 192 | aes 256}`	IKE ポリシーでの暗号化アルゴリズムを指定します。 • **aes** : 暗号化アルゴリズムとして 128 ビット AES を指定します。 • **aes 192** : 暗号化アルゴリズムとして 192 ビット AES を指定します。 • **aes 256** : 暗号化アルゴリズムとして 256 ビット AES を指定します。
ステップ 3	`...` `Router(config-isakmp)# exit`	必要に応じてその他のポリシー値を指定したあと、ISAKMP ポリシー コンフィギュレーション モードを終了します。 ISAKMP ポリシーの設定についての詳細は、『*Cisco IOS Security Configuration Guide*』を参照してください。

AES IKE ポリシーの確認

AES IKE ポリシーの設定を確認するには、**show crypto isakmp policy** コマンドを入力します。

```
Router# show crypto isakmp policy

Protection suite of priority 1
encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
hash algorithm:        Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group:  #1 (768 bit)
lifetime: 3600 seconds, no volume limit

Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

AES の設定例は、「AES の設定例」（P.27-22）を参照してください。

ISAKMP キーリングの設定

暗号キーリングは事前共有キーと RSA パブリック キーの集合体です。キーリングを設定して ISAKMP プロファイルに関連付けることができます。暗号 ISAKMP プロファイルには、0、1、または複数のキーリングを含めることができます。

ISAKMP キーリング機能（別名、SafeNet IPSec VPN クライアント サポート機能）を使用すると、**local-address** コマンドを使用して ISAKMP プロファイルまたは ISAKMP キーリング設定の適用範囲をローカルな終端アドレスまたはインターフェイスに限定できます。この機能のメリットは、異なるローカル終端アドレスを使用することで、異なるユーザが同じピア アイデンティティおよび ISAKMP キーを使用できる点です。

ISAKMP キーリング設定時の注意事項および制約事項

ISAKMP キーリングを設定する場合は、次の注意事項および制約事項に従ってください。

- ローカル アドレス オプションは、インターフェイスのプライマリ アドレスにだけ使用できます。
- IP アドレスを割り当てる場合、割り当てたアドレスで確実にピアの接続を終端する必要があります。
- デバイスに IP アドレスが存在しない場合、またはインターフェイスに IP アドレスがない場合には、ISAKMP プロファイルまたは ISAKMP キーリングは実質的にディセーブルになります。

ローカル終端アドレスまたはインターフェイスへの ISAKMP プロファイルの限定

ISAKMP プロファイルを設定し、そのプロファイルをローカル終端アドレスまたはインターフェイスに限定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto isakmp profile profile-name`	ISAKMP プロファイルを定義し、ISAKMP 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。 • *profile-name*：ISAKMP プロファイルの名前。
ステップ 2	`Router(conf-isa-profile)# keyring keyring-name`	（任意）ISAKMP プロファイルとともにキーリングを設定します。 • *keyring-name*：暗号キーリングの名前。 **（注）** ISAKMP プロファイル内にキーリングがなくても、ローカル終端は動作します。Rivest, Shamir, and Adelman（RSA）証明書を使用する場合にも、ローカル終端は動作します。

	コマンド	説明
ステップ 3	`Router(conf-isa-profile)# match identity address address`	ピアからのアイデンティティを ISAKMP プロファイルと照合します。 • *address*：リモート ピアの IP アドレス。
ステップ 4	`Router(conf-isa-profile)# local-address {interface-name | ip-address [vrf-tag]}`	ISAKMP プロファイルまたは ISAKMP キーリング設定の適用範囲を、ローカルな終端アドレスまたはインターフェイスに限定します。 • *interface-name*：ローカル インターフェイスの名前。 • *ip-address*：ローカル終端アドレス。 • *vrf-tag*：（任意）IP アドレスの適用範囲を VRF に限定します。

ローカル終端アドレスまたはインターフェイスへのキーリングの限定

ISAKMP キーリングを設定し、その適用範囲をローカル終端アドレスまたはインターフェイスに限定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# keyring keyring-name`	IKE 認証時に使用する暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。 • *keyring-name*：暗号キーリングの名前。
ステップ 2	`Router(conf-keyring)# local-address {interface-name | ip-address [vrf-tag]}`	ISAKMP プロファイルまたは ISAKMP キーリング設定の適用範囲を、ローカルな終端アドレスまたはインターフェイスに限定します。 • *interface-name*：ローカル インターフェイスの名前。 • *ip-address*：ローカル終端アドレス。 • *vrf-tag*：（任意）IP アドレスの適用範囲を VRF に限定します。
ステップ 3	`Router(conf-keyring)# pre-shared-key address address`	IKE 認証に使用する事前共有キーを定義します。 • *address*：IP アドレス

SafeNet IPSec VPN クライアントのサポートに関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_scse.html

ISAKMP キーリングの設定例は、「ISAKMP キーリングの設定例」（P.27-22）を参照してください。

証明書/ISAKMP プロファイル マッピングの設定

証明書/ISAKMP プロファイル マッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに ISAKMP プロファイルを割り当てることができます。また、ISAKMP プロファイルに割り当てられたピアにグループ名を割り当てることもできます。

（注）　証明書/ISAKMP プロファイル マッピングは、Cisco IOS Release 12.2(33)SRA 以降でのみサポートされています。

証明書/ISAKMP プロファイル マッピング設定時の注意事項および制約事項

証明書/ISAKMP プロファイル マッピングを設定する場合は、次の注意事項および制約事項に従ってください。

- 証明書を交換しないで、RSA シグニチャまたは RSA 暗号化認証を使用する場合は、この機能を適用できません。ISAKMP ピアは、証明書を使用して RSA シグニチャまたは RSA 暗号化認証を実行するように設定する必要があります。

証明書/ISAKMP プロファイル マッピング

証明書と ISAKMP プロファイルをマッピングするには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto isakmp profile profile-name`	ISAKMP プロファイルを定義し、ISAKMP 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。 • *profile-name*：ユーザ プロファイルの名前。
ステップ 2	`Router(config-isa-prof)# match certificate certificate-map`	証明書マップの名前を受け入れます。 • *certificate-map*：証明書マップの名前。

証明書/ISAKMP プロファイル マッピング設定の確認

証明書マップの件名が適切に設定されているか確認するには、**show crypto pki certificates** コマンドおよび **debug crypto isakmp** コマンドを使用します。

show crypto pki certificates コマンドは、ピアの現在の IKE SA をすべて表示します。**debug crypto isakmp** コマンドでは、IKE イベントに関するメッセージが表示されます。

次に、証明書が ISAKMP プロファイルにマッピングされている例を示します。この例には、応答側と発信側の設定､証明書マップの件名が設定されているかを確認するための **show crypto pki certificates** コマンドの出力、および証明書に証明書マップ照合を行い、ISAKMP プロファイルと照合したことを示す **debug crypto isakmp** コマンドの出力が含まれます。

応答側の設定

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
 subject-name co ou = green
! The above line shows that the subject name must have "ou = green."
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
of the peer matches cert_map (shown on third line below).
   ca trust-point 2315
   ca trust-point LaBcA
```

```
   match certificate cert_map
```

発信側の設定

```
crypto ca trustpoint LaBcA
 enrollment url http://10.76.82.20:80/cgi-bin/openscep
 subject-name ou=green,c=IN
! The above line ensures that the subject name "ou = green" is set.
 revocation-check none
```

発信側の show crypto pki certificates コマンド出力

```
Router# show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number: 21
  Certificate Usage: General Purpose
  Issuer:
    cn=blue-lab CA
    o=CISCO
    c=IN
  Subject:
    Name: Router.cisco.com
    c=IN
    ou=green
! The above line is a double check that "ou = green" has been set as the subject name.
    hostname=Router.cisco.com
  Validity Date:
    start date: 14:34:30 UTC Mar 31 2004
    end   date: 14:34:30 UTC Apr 1 2009
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: LaBcA
```

応答側の debug crypto isakmp コマンド出力

```
Router# debug crypto isakmp

*Nov  6 19:31:25.010: ISAKMP:(0): SA request profile is prof2
*Nov  6 19:31:25.010: ISAKMP: Found a peer struct for 14.0.0.2, peer port 500
*Nov  6 19:31:25.010: ISAKMP: Locking peer struct 0x13884FB8, refcount 349 for
isakmp_initiator
*Nov  6 19:31:25.010: ISAKMP[I]: sa->swdb: Vlan3
*Nov  6 19:31:25.010: ISAKMP: local port 500, remote port 500
*Nov  6 19:31:25.010: ISAKMP: set new node 0 to QM_IDLE
*Nov  6 19:31:25.010: ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa
= 13C041E8
*Nov  6 19:31:25.010: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
*Nov  6 19:31:25.010: ISAKMP:(0):Profile has no keyring, aborting key search
*Nov  6 19:31:25.010: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Nov  6 19:31:25.010: ISAKMP:(0): constructed NAT-T vendor-03 ID
*Nov  6 19:31:25.010: ISAKMP:(0): constructed NAT-T vendor-02 ID
*Nov  6 19:31:25.010: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
*Nov  6 19:31:25.010: ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1

*Nov  6 19:31:25.010: ISAKMP:(0): beginning Main Mode exchange
*Nov  6 19:31:25.010: ISAKMP:(0): sending packet to 14.0.0.2 my_port 500 peer_port 500 (I)
MM_NO_STATE
*Nov  6 19:31:25.018: ISAKMP (0): received packet from 14.0.0.2 dport 500 sport 500 fvrf
(N) NEW SA
*Nov  6 19:31:25.018: ISAKMP: Found a peer struct for 14.0.0.2, peer port 500
```

```
*Nov  6 19:31:25.018: ISAKMP: Locking peer struct 0x13884FB8, refcount 350 for
crypto_isakmp_process_block
*Nov  6 19:31:25.018: ISAKMP[R]: sa->swdb: Vlan2
*Nov  6 19:31:25.018: ISAKMP: local port 500, remote port 500
*Nov  6 19:31:25.018: ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa
= 148C68D8
*Nov  6 19:31:25.018: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Nov  6 19:31:25.018: ISAKMP:(0):Old State = IKE_READY  New State = IKE_R_MM1

*Nov  6 19:31:25.018: ISAKMP:(0): processing SA payload. message ID = 0
*Nov  6 19:31:25.018: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.018: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
*Nov  6 19:31:25.018: ISAKMP (0): vendor ID is NAT-T v7
*Nov  6 19:31:25.018: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.018: ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
*Nov  6 19:31:25.018: ISAKMP:(0): vendor ID is NAT-T v3
*Nov  6 19:31:25.018: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.018: ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
*Nov  6 19:31:25.018: ISAKMP:(0): vendor ID is NAT-T v2
*Nov  6 19:31:25.038: ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
*Nov  6 19:31:25.038: ISAKMP:      encryption 3DES-CBC
*Nov  6 19:31:25.038: ISAKMP:      hash MD5
*Nov  6 19:31:25.038: ISAKMP:      default group 1
*Nov  6 19:31:25.038: ISAKMP:      auth RSA sig
*Nov  6 19:31:25.038: ISAKMP:      life type in seconds
*Nov  6 19:31:25.038: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Nov  6 19:31:25.042: ISAKMP:(0):atts are acceptable. Next payload is 3
*Nov  6 19:31:25.042: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.042: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
*Nov  6 19:31:25.042: ISAKMP (0): vendor ID is NAT-T v7
*Nov  6 19:31:25.042: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.042: ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
*Nov  6 19:31:25.042: ISAKMP:(0): vendor ID is NAT-T v3
*Nov  6 19:31:25.042: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.042: ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
*Nov  6 19:31:25.042: ISAKMP:(0): vendor ID is NAT-T v2
*Nov  6 19:31:25.042: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Nov  6 19:31:25.042: ISAKMP:(0):Old State = IKE_R_MM1  New State = IKE_R_MM1

*Nov  6 19:31:25.046: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Nov  6 19:31:25.046: ISAKMP:(0): sending packet to 14.0.0.2 my_port 500 peer_port 500 (R)
MM_SA_SETUP
*Nov  6 19:31:25.046: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Nov  6 19:31:25.046: ISAKMP:(0):Old State = IKE_R_MM1  New State = IKE_R_MM2

*Nov  6 19:31:25.046: ISAKMP (0): received packet from 14.0.0.2 dport 500 sport 500 fvrf
(I) MM_NO_STATE
*Nov  6 19:31:25.046: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Nov  6 19:31:25.046: ISAKMP:(0):Old State = IKE_I_MM1  New State = IKE_I_MM2

*Nov  6 19:31:25.046: ISAKMP:(0): processing SA payload. message ID = 0
*Nov  6 19:31:25.046: ISAKMP:(0): processing vendor id payload
*Nov  6 19:31:25.046: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
*Nov  6 19:31:25.046: ISAKMP (0): vendor ID is NAT-T v7
*Nov  6 19:31:25.046: ISAKMP : Looking for xauth in profile prof2
*Nov  6 19:31:25.046: ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
*Nov  6 19:31:25.046: ISAKMP:      encryption 3DES-CBC
*Nov  6 19:31:25.046: ISAKMP:      hash MD5
*Nov  6 19:31:25.046: ISAKMP:      default group 1
*Nov  6 19:31:25.046: ISAKMP:      auth RSA sig
*Nov  6 19:31:25.050: ISAKMP:      life type in seconds
*Nov  6 19:31:25.050: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Nov  6 19:31:25.050: ISAKMP:(0):atts are acceptable. Next payload is 0
*Nov  6 19:31:25.050: ISAKMP:(0): processing vendor id payload
```

```
*Nov  6 19:31:25.050: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
*Nov  6 19:31:25.050: ISAKMP (0): vendor ID is NAT-T v7
*Nov  6 19:31:25.050: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Nov  6 19:31:25.050: ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM2

*Nov  6 19:31:25.050: ISAKMP (0): constructing CERT_REQ for issuer
cn=mscavpn1,ou=isbu,o=cisco
*Nov  6 19:31:25.054: ISAKMP:(0): sending packet to 14.0.0.2 my_port 500 peer_port 500 (I)
MM_SA_SETUP
*Nov  6 19:31:25.054: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Nov  6 19:31:25.054: ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3

*Nov  6 19:31:25.058: ISAKMP (0): received packet from 14.0.0.2 dport 500 sport 500 fvrf
(R) MM_SA_SETUP
*Nov  6 19:31:25.062: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Nov  6 19:31:25.062: ISAKMP:(0):Old State = IKE_R_MM2  New State = IKE_R_MM3

*Nov  6 19:31:25.062: ISAKMP:(0): processing KE payload. message ID = 0
*Nov  6 19:31:25.062: ISAKMP:(0): processing NONCE payload. message ID = 0
*Nov  6 19:31:25.062: ISAKMP:(83727): processing CERT_REQ payload. message ID = 0
*Nov  6 19:31:25.062: ISAKMP:(83727): peer wants a CT_X509_SIGNATURE cert
*Nov  6 19:31:25.066: ISAKMP:(83727): peer want cert issued by cn=mscavpn1,ou=isbu,o=cisco
*Nov  6 19:31:25.066: ISAKMP:(83727): Choosing trustpoint MSCA as issuer
*Nov  6 19:31:25.066: ISAKMP:(83727): processing vendor id payload
*Nov  6 19:31:25.066: ISAKMP:(83727): vendor ID is DPD
*Nov  6 19:31:25.066: ISAKMP:(83727): processing vendor id payload
*Nov  6 19:31:25.066: ISAKMP:(83727): speaking to another IOS box!
*Nov  6 19:31:25.066: ISAKMP:(83727): processing vendor id payload
*Nov  6 19:31:25.066: ISAKMP:(83727): vendor ID seems Unity/DPD but major 230 mismatch
*Nov  6 19:31:25.066: ISAKMP:(83727): vendor ID is XAUTH
*Nov  6 19:31:25.066: ISAKMP (83727): His hash no match - this node outside NAT
*Nov  6 19:31:25.066: ISAKMP (83727): No NAT Found for self or peer
*Nov  6 19:31:25.066: ISAKMP:(83727):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Nov  6 19:31:25.066: ISAKMP:(83727):Old State = IKE_R_MM3  New State = IKE_R_MM3

*Nov  6 19:31:25.066: ISAKMP (83727): constructing CERT_REQ for issuer
cn=mscavpn1,ou=isbu,o=cisco
*Nov  6 19:31:25.066: ISAKMP:(83727): sending packet to 14.0.0.2 my_port 500 peer_port 500
(R) MM_KEY_EXCH
*Nov  6 19:31:25.070: ISAKMP:(83727):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Nov  6 19:31:25.070: ISAKMP:(83727):Old State = IKE_R_MM3  New State = IKE_R_MM4

*Nov  6 19:31:25.070: ISAKMP (0): received packet from 14.0.0.2 dport 500 sport 500 fvrf
(I) MM_SA_SETUP
*Nov  6 19:31:25.070: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Nov  6 19:31:25.070: ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4

*Nov  6 19:31:25.070: ISAKMP:(0): processing KE payload. message ID = 0
*Nov  6 19:31:25.074: ISAKMP:(0): processing NONCE payload. message ID = 0
*Nov  6 19:31:25.098: ISKAMP: growing send buffer from 1024 to 3072

*Nov  6 19:31:25.118: ISAKMP (83727): received packet from 14.0.0.2 dport 500 sport 500
fvrf (R) MM_KEY_EXCH
*Nov  6 19:31:25.122: ISAKMP:(83727):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Nov  6 19:31:25.122: ISAKMP:(83727):Old State = IKE_R_MM4  New State = IKE_R_MM5

*Nov  6 19:31:25.122: ISAKMP:(83727): processing ID payload. message ID = 0
*Nov  6 19:31:25.122: ISAKMP (83727): ID payload
        next-payload : 6
        type         : 3
        USER FQDN    : a@vrf2.com
        protocol     : 17
        port         : 500
        length       : 18
```

```
*Nov  6 19:31:25.134: ISAKMP:(83727):: peer matches prof2 profile
*Nov  6 19:31:25.134: ISAKMP:(83727): processing CERT payload. message ID = 0
*Nov  6 19:31:25.134: ISAKMP:(83727): processing a CT_X509_SIGNATURE cert
*Nov  6 19:31:25.142: ISAKMP:(83727): peer's pubkey isn't cached
*Nov  6 19:31:25.158: %CRYPTO-6-IKMP_NO_ID_CERT_USER_FQDN_MATCH: ID of a@vrf2.com (type 3)
and certificate user fqdn with empty
*Nov  6 19:31:25.158: ISAKMP (83727): adding peer's pubkey to cache
*Nov  6 19:31:25.158: ISAKMP:(83727): processing SIG payload. message ID = 0
*Nov  6 19:31:25.162: ISAKMP:(83727):SA authentication status:
        authenticated
*Nov  6 19:31:25.162: ISAKMP:(83727):SA has been authenticated with 14.0.0.2
*Nov  6 19:31:25.162: ISAKMP:(83727):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Nov  6 19:31:25.162: ISAKMP:(83727):Old State = IKE_R_MM5  New State = IKE_R_MM5

*Nov  6 19:31:25.170: ISAKMP:(83727):SA is doing RSA signature authentication using id
type ID_USER_FQDN
*Nov  6 19:31:25.170: ISAKMP (83727): ID payload
        next-payload : 6
        type         : 3
        USER FQDN    : a@vrf2.com
        protocol     : 17
        port         : 500
        length       : 18
*Nov  6 19:31:25.170: ISAKMP:(83727):Total payload length: 18
*Nov  6 19:31:25.182: ISAKMP (83727): constructing CERT payload for
cn=HUB,ou=isbu,o=cisco,hostname=HUB.cisco.com,serialNumber=1234D
*Nov  6 19:31:25.182: ISKAMP: growing send buffer from 1024 to 3072
*Nov  6 19:31:25.186: ISAKMP:(83727): using the MSCA trustpoint's keypair to sign
*Nov  6 19:31:25.194: ISAKMP:(83727): sending packet to 14.0.0.2 my_port 500 peer_port 500
(R) MM_KEY_EXCH
*Nov  6 19:31:25.198: ISAKMP:(83727):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Nov  6 19:31:25.198: ISAKMP:(83727):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

*Nov  6 19:31:25.198: ISAKMP:(83727):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Nov  6 19:31:25.198: ISAKMP:(83727):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE

*Nov  6 19:31:25.238: ISAKMP (83727): received packet from 14.0.0.2 dport 500 sport 500
fvrf (R) QM_IDLE
*Nov  6 19:31:25.238: ISAKMP: set new node -134314170 to QM_IDLE
*Nov  6 19:31:25.242: ISAKMP:(83727): processing HASH payload. message ID = -134314170
*Nov  6 19:31:25.242: ISAKMP:(83727): processing SA payload. message ID = -134314170
*Nov  6 19:31:25.242: ISAKMP:(83727):Checking IPSec proposal 1
*Nov  6 19:31:25.242: ISAKMP: transform 1, ESP_3DES
*Nov  6 19:31:25.242: ISAKMP:   attributes in transform:
*Nov  6 19:31:25.242: ISAKMP:      encaps is 1 (Tunnel)
*Nov  6 19:31:25.242: ISAKMP:      SA life type in seconds
*Nov  6 19:31:25.242: ISAKMP:      SA life duration (basic) of 3600
*Nov  6 19:31:25.242: ISAKMP:      SA life type in kilobytes
*Nov  6 19:31:25.242: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Nov  6 19:31:25.242: ISAKMP:      authenticator is HMAC-SHA
*Nov  6 19:31:25.242: ISAKMP:(83727):atts are acceptable.
*Nov  6 19:31:25.242: ISAKMP:(83727): processing NONCE payload. message ID = -134314170
*Nov  6 19:31:25.242: ISAKMP:(83727): processing ID payload. message ID = -134314170
*Nov  6 19:31:25.242: ISAKMP:(83727): processing ID payload. message ID = -134314170
*Nov  6 19:31:25.242: ISAKMP:(83727):QM Responder gets spi
*Nov  6 19:31:25.242: ISAKMP:(83727):Node -134314170, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
*Nov  6 19:31:25.242: ISAKMP:(83727):Old State = IKE_QM_READY  New State =
IKE_QM_SPI_STARVE
*Nov  6 19:31:25.242: ISAKMP:(83727): Creating IPSec SAs
*Nov  6 19:31:25.246:         inbound SA from 14.0.0.2 to 15.0.0.2 (f/i)  1/714
        (proxy 12.0.0.2 to 13.0.0.2)
*Nov  6 19:31:25.246:         has spi 0x917AD879 and conn_id 0
```

```
*Nov  6 19:31:25.246:         lifetime of 3600 seconds
*Nov  6 19:31:25.246:         lifetime of 4608000 kilobytes
*Nov  6 19:31:25.246:         outbound SA from 15.0.0.2 to 14.0.0.2 (f/i) 1/714
        (proxy 13.0.0.2 to 12.0.0.2)
*Nov  6 19:31:25.246:         has spi  0xC54A5A05 and conn_id 0
*Nov  6 19:31:25.246:         lifetime of 3600 seconds
*Nov  6 19:31:25.246:         lifetime of 4608000 kilobytes
*Nov  6 19:31:25.246:  ISAKMP: Failed to find peer index node to update peer_info_list
*Nov  6 19:31:25.250: ISAKMP:(83727): sending packet to 14.0.0.2 my_port 500 peer_port 500
(R) QM_IDLE
*Nov  6 19:31:25.250: ISAKMP:(83727):Node -134314170, Input = IKE_MESG_INTERNAL,
IKE_GOT_SPI
*Nov  6 19:31:25.250: ISAKMP:(83727):Old State = IKE_QM_SPI_STARVE  New State =
IKE_QM_R_QM2
*Nov  6 19:31:25.270: ISAKMP (83727): received packet from 14.0.0.2 dport 500 sport 500
fvrf (R) QM_IDLE
*Nov  6 19:31:25.274: ISAKMP:(83727):deleting node -134314170 error FALSE reason "QM done
(await)"
*Nov  6 19:31:25.274: ISAKMP:(83727):Node -134314170, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
*Nov  6 19:31:25.274: ISAKMP:(83727):Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
*Nov  6 19:32:15.282: ISAKMP:(83727):purging node -134314170
```

応答側の show crypto isakmp sa [detail] コマンド出力

```
Router# show crypto isakmp sa vrf vrf2
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
15.0.0.2        14.0.0.2        QM_IDLE          83727 ACTIVE prof2

IPv6 Crypto ISAKMP SA

Router# show crypto isakmp sa detail vrf vrf2
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.

83727 15.0.0.2        14.0.0.2        vrf2     ACTIVE 3des md5  rsig 1  23:59:15
       Engine-id:Conn-id =  :15727

IPv6 Crypto ISAKMP SA
```

ピアへのグループ名の割り当て

ピアに割り当てる ISAKMP プロファイルにグループ名を対応付けるには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	説明
ステップ 1	`Router(config)# crypto isakmp profile profile-name`	ISAKMP プロファイルを定義し、ISAKMP 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。 • *profile-name*：ユーザ プロファイルの名前。
ステップ 2	`Router (conf-isa-prof)# client configuration group group-name`	ピアにこの暗号 ISAKMP プロファイルが割り当てられている場合、ピアに割り当てられるグループ名を受け入れます。 • *group-name*：ピアに対応付けられるグループ名。

グループ名とピアの割り当て設定の確認

グループ名がピアに割り当てられていることを確認するには、**debug crypto isakmp** コマンドを入力します。

debug crypto isakmp コマンドでは、IKE イベントに関するメッセージが表示されます。

次の **debug crypto isakmp** コマンドの出力は、ピアが ISAKMP プロファイル「certpro」と照合され、グループ名「new_group」が割り当てられたことを示します。

発信側の設定

```
crypto isakmp profile certpro
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   client configuration group new_group
! The statement on the above line will assign the group "new_group" to any peer that
matches the ISAKMP profile "certpro."
   initiate mode aggressive
```

応答側の debug crypto isakmp コマンド出力

```
Router# debug crypto isakmp
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : Router1.cisco.com
        protocol     : 17
```

```
        port         : 500
        length       : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group
```

証明書/ISAKMP プロファイル マッピングに関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_isakp.html

証明書/ISAKMP プロファイル マッピングの設定例は、「証明書/ISAKMP プロファイル マッピングの設定例」（P.27-23）を参照してください。

暗号化事前共有キーの設定

暗号化事前共有キー機能を使用すると、平文のパスワードをタイプ 6（暗号化）フォーマットで NVRAM に安全に保管できます。

暗号化事前共有キー設定時の注意事項および制約事項

暗号化事前共有キーを設定する場合は、次の注意事項および制約事項に従ってください。

- 古い ROM モニタ（ROMMON）およびブート イメージでは、新しいタイプ 6 パスワードが認識されません。古い ROMMON から起動すると、エラーが表示される可能性があります。
- **key config-key password-encryption** コマンドを使用して、パスワード（マスター キー）が変更または再暗号化されると、タイプ 6 の暗号化を使用するアプリケーション モジュールに、リストレジストリによって古いキーと新しいキーが渡されます。
- **key config-key password-encryption** コマンドを使用して設定したマスター キーがシステムから削除されると、すべてのタイプ 6 パスワードが無効になるという警告が生成されます（確認のプロンプトも表示されます）。セキュリティを確保するため、暗号化されたパスワードが Cisco IOS ソフトウェアによって復号化されることはありません。ただし、パスワードの再暗号化は可能です。

注意　**key config-key password-encryption** コマンドで設定したパスワードを忘れた場合、そのパスワードを回復することはできません。パスワードは安全な場所に保管してください。

- あとの段階で **no password encryption aes** コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encryption** コマンドを使用して設定したパスワード（マスター キー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。
- （**key config-key password-encryption** コマンドで設定した）パスワードは「解読不能」のため、ルータからパスワードを取得する方法はありません。既存の管理ステーションは、パスワードを「知ることができません」。別の場所にパスワードを保存するように管理ステーションの機能を拡張すれば別ですが、その場合には管理システム内にパスワードを安全に保存する必要があります。TFTP（簡易ファイル転送プロトコル）を使用してコンフィギュレーションを保存する場合、その

コンフィギュレーションはスタンドアロンではないため、ルータにロードすることはできません。コンフィギュレーションをルータにロードする前後には、（**key config-key password-encryption** コマンドを使用して）パスワードを手動で追加する必要があります。パスワードは保存されたコンフィギュレーションに手動で追加することはできますが、この場合、そのコンフィギュレーションのすべてのパスワードを誰でも復号化できるようになるため推奨できません。

- マスター キーと一致しない暗号テキストを入力またはカットアンドペーストした場合、またはマスター キーが存在しない場合、その暗号テキストは許可されるか保存されますが、次のアラートメッセージが出力されます。

  ```
  ciphertext>[for username bar>] is incompatible with the configured master key
  ```

- 新しいマスター キーを設定すると、すべての平文のキーが暗号化され、タイプ 6 キーになります。既存のタイプ 6 キーは暗号化されません。既存のタイプ 6 キーはそのまま残されます。
- 古いマスター キーを忘れたり、不明な場合は、**no key config-key password-encryption** コマンドを使用して、そのマスター キーを削除できます。**no key config-key password-encryption** コマンドを使用してマスター キーを削除すると、既存の暗号化パスワードはルータ コンフィギュレーションに暗号化されたまま残ります。これらのパスワードは復号化されません。

暗号化事前共有キーの設定

暗号化事前共有キーを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明

ステップ 1	`Router(config)# key config-key password-encryption`	プライベート NVRAM にタイプ 6 暗号キーを保存します。
		次の事項に注意してください。
		• キーを対話形式で入力（**Enter** キーを使用）し、暗号キーがすでに存在している場合、次のプロンプトが表示されます。
		`Old key, New key, and Confirm key`
		• キーを対話形式で入力し、暗号キーが存在しない場合、次のプロンプトが表示されます。
		`New key and Confirm key`
		• すでに暗号化されているパスワードを削除しようとすると、次のプロンプトが表示されます。
		`WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:`

ステップ 2	`Router(config)# password-encryption aes`	暗号化事前共有キーをイネーブルにします。

暗号化事前共有キーの設定の確認

新しいマスター キーが設定され、その新しいマスター キーを使用してキーが暗号化されたことを確認するには、**password logging** コマンドを使用します。以下に、このコマンドの出力例を示します。

```
Router(config)# password logging
```

```
Router(config)# key config-key password-encrypt

New key:
Confirm key:
Router(config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas

Router(config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

暗号化事前共有キー機能に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_epsk.html

暗号化事前共有キーの設定例は、「暗号化事前共有キーの設定例」（P.27-23）を参照してください。

IKE の CAC の設定

IKE の CAC（コール アドミッション制御）を使用すると、ルータが同時に確立できる IKE SA 数を制限できます。

（注）　コール アドミッション制御は、Cisco IOS Release 12.2(33)SRA 以降のリリースでサポートされます。

ルータ間に確立できる IKE SA 数は、次の 2 つの方法で制限できます。

- **crypto call admission limit** コマンドを入力して、絶対的な IKE SA 制限を設定します。

  IKE SA 制限が定義されている場合に、制限値に達すると、ルータでは、次のように新しい IKE SA 要求が受け入れまたは開始されなくなります。ピア ルータから新しい SA 要求が送信された場合、IKE はアクティブな IKE SA 数とネゴシエーション中の SA 数の合計が、設定された SA 制限に適合しているか、または超過しているかを判別します。合計数が制限値以上である場合、新しい SA 要求は拒否され、Syslog が生成されます。このログには、SA 要求の送信元/宛先 IP アドレスが格納されます。

- **call admission limit** コマンドを入力して、システム リソース制限を設定します。

  システム リソース制限が定義されている場合に、使用中のシステム リソースが指定レベルに達すると、ルータでは、次のように新しい IKE SA 要求が受け入れまたは開始されなくなります。CAC はグローバル リソース モニタをポーリングして、ルータの CPU サイクルまたはメモリ バッファが不足する時期を IKE が把握できるようにします。リソース制限には、システム リソースのレベルを表す 1 ～ 100000 の値を設定できます。このレベルのシステム リソースが使用されている場合、IKE は 新しい IKE SA 要求を受け入れまたは開始しなくなります。

CAC は新しい SA（ピア間に SA が存在しない場合）および再生成 SA キーに適用されます。既存 SA を保護するためにあらゆる作業が行われます。システム リソースが不足している場合、または設定された IKE SA 制限に達した場合は、新しい SA 要求だけが拒否されます。

IKE SA 制限の設定

IKE SA 制限を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。IKE SA 制限が定義されている場合に、この制限に達すると、ルータでは、次のように新しい IKE SA 要求が受け入れまたは開始されなくなります。

	コマンド	説明
ステップ 1	`Router(config)# crypto call admission limit {ike {sa number | in-negotiation-sa number}}`	IKE が新しい SA 要求を受け入れまたは開始しなくなるまでにルータが確立できる IKE SA の最大数を指定します。 • **sa** *number*：ルータで許可されるアクティブな IKE SA の数。範囲は 0 ～ 99999 です。 • **in-negotiation-sa** *number*：ルータでネゴシエーションされる IKE SA の数。範囲は 10 ～ 99999 です。 **（注）** ISAKMP 接続は 2 方向で確立される必要があります。ネットワークに 500 スポークがある場合、この値を最小で 1000（500 x 2）に設定する必要があります。
ステップ 2	`Router(config)# exit`	特権 EXEC モードに戻ります。

システム リソース制限の設定

システム リソース制限を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。IKE SA の制限が定義されている場合に、使用中のシステム リソースが指定レベルに達すると、ルータでは、新しい IKE SA 要求が受け入れまたは開始されなくなります。

	コマンド	説明
ステップ 1	`Router(config)# call admission limit charge`	指定されたレベルのシステム リソースが使用されている場合に、新しい SA（セキュリティ アソシエーション）要求の開始または受け入れを停止するように IKE に指示します（CAC（コール アドミッション制御）を要求します）。 • *charge*：システム リソースのレベル。この値が使用されている場合、IKE は新しい SA 要求の受け入れを停止します。有効値は、1 ～ 100000 です。
ステップ 2	`Router(config)# exit`	特権 EXEC モードに戻ります。

CAC 統計情報のクリア

許可または拒否された IKE 要求数を追跡する CAC カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear crypto call admission statistics** コマンドを使用します。

```
Router(config)# clear crypto call admission statistics
```

IKE の CAC の設定確認

CAC が設定されているか確認するには、**show call admission statistics** コマンドおよび **show crypto call admission statistics** コマンドを使用します。

show call admission statistics コマンドは、グローバルな CAC 設定パラメータおよび CAC の動作をモニタします。

```
Router# show call admission statistics
Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

show crypto call admission statistics コマンドは、暗号 CAC 統計情報をモニタします。

```
Router# show crypto call admission statistics
----------------------------------------------------------
               Crypto Call Admission Control Statistics
----------------------------------------------------------
System Resource Limit: 0    Max IKE SAs 0
Total IKE SA Count:    0    active:     0   negotiating: 0
Incoming IKE Requests: 0    accepted:   0   rejected:    0
Outgoing IKE Requests: 0    accepted:   0   rejected:    0
Rejected IKE Requests: 0    rsrc low:   0   SA limit:    0
```

IKE の CAC に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtcallik.html

IKE の CAC の設定例は、「IKE の CAC の設定例」（P.27-24）を参照してください。

DPD の設定

RFC 3706 で定義されている Dead Peer Detection（DPD）は、動作していない IPSec ピアを検出するためのメカニズムです。IPSec はピアツーピア タイプのテクノロジーです。ルーティングの問題やピアのリロードなどのために、ピア間の IP 接続が切断される場合があります。このような接続の切断があると、トラフィックが消失するブラック ホール状態を引き起こします。トラフィック検出方式に基づく DPD は、このような状況に対処するためのメカニズムの 1 つです。

（注）　**crypto isakmp keepalive** コマンドの **periodic** オプションは、Cisco IOS Release 12.2(33)SRA でのみサポートされます。**on-demand** オプションは、すべてのリリースでサポートされています。

DPD は、on-demand または periodic の 2 つのオプションをサポートします。オンデマンド方式がデフォルトです。オンデマンド DPD の場合、メッセージはトラフィック パターンに基づいて送信されます。たとえば、ルータが発信トラフィックを送信する必要があるときに、ピアが存続しているかどうか不明である場合、ルータは DPD メッセージを送信して、ピアのステータスを問い合わせます。ルータに送信すべきトラフィックがない場合、DPD メッセージは送信されません。ピアが停止していて、ピアに送信するトラフィックがルータに存在しない場合、IKE または IPSec SA がキーを再生成する必要が生じるまで、ルータは判別しません（ルータがピアと通信しようとしていない場合、ピアが存続するかどうかは重要でありません）。一方、ピアに送信するトラフィックがルータに存在するにもかかわらず、ピアが応答しない場合、ルータは DPD メッセージを送信して、ピアの状態を判別します。

定期方式の場合は、定期的に DPD メッセージを「強制送信」するように、ルータを設定できます。この強制方式では、停止したピアが早期に検出されます。たとえば、ルータに送信するトラフィックがない場合も、DPD メッセージは定期的に送信されます。ピアが停止している場合、ルータは IKE SA がタイムアウトして判別を開始するまで待機する必要はありません。

DPD を設定するには、**crypto isakmp keepalive** コマンドを使用します。DPD および Cisco IOS キープアライブは、タイマーに基づいて機能します。タイマーが 10 秒に設定されている場合、ルータは「hello」メッセージを 10 秒おきに送信します（ルータが「hello」メッセージをピアから受信する場合を除く）。Cisco IOS キープアライブおよび定期的 DPD の利点は、停止したピアを早期に検出できることです。ただし、Cisco IOS キープアライブおよび定期的 DPD を利用するには、定期メッセージの送信頻度を高める必要があります。メッセージの送信頻度が高くなると、通信中のピアはより多くのパケットを暗号化および復号化する必要があります。

暗号マップ内で DPD および Cisco IOS キープアライブ機能を複数のピアと組み合わせることにより、ステートレス フェールオーバーを実現できます。DPD を使用すると、ルータは停止した IKE ピアを検出できます。停止状態を検出したルータは、ピアに対する IPSec および IKE SA を削除します。複数のピアが構成されている場合、ルータは一覧内の次のピアにスイッチオーバーして、ステートレス フェールオーバーを実現します。

DPD 設定時の注意事項および制約事項

DPD を設定する場合は、次の注意事項および制約事項に従ってください。

- **crypto isakmp keepalive** コマンドを設定すると、Cisco IOS ソフトウェアは、ピアがサポートしているプロトコルに応じて、Cisco IOS キープアライブまたは DPD の使用についてネゴシエートを行います。
- **crypto isakmp keepalive** コマンドを使用して **periodic** オプションを設定しない場合、ルータのデフォルトは **on-demand** 方式になります。
- 定期的 DPD を設定する前に、IKE ピアが DPD をサポートしていることを確認する必要があります。DPD をサポートしているのは、Cisco VPN 3000 コンセントレータ、Cisco PIX ファイアウォール、Cisco VPN クライアント、およびすべての動作モードの Cisco IOS ソフトウェア（サイト間、Easy VPN リモート、Easy VPN サーバ）などです。
- 定期的 DPD を使用した場合、ルータはオンデマンド DPD よりも短い応答時間で、応答しない IKE ピアを検出できます。ただし、定期的 DPD を使用すると余分なオーバーヘッドが発生します。多数の IKE ピアと通信する場合は、代わりにオンデマンド DPD を使用することを検討してください。
- **crypto isakmp keepalive** *seconds* コマンドを使用して DPD を設定する場合、*seconds* 引数は DPD メッセージ間の間隔を指定します。オンデマンド DPD の場合、実間隔は最大で設定値の 2 倍までになることがあります。

DPD メッセージの設定

ルータが DPD メッセージをピアに送信できるようにするには、次の作業を行います。

コマンド	説明
Router# **crypto isakmp keepalive** *seconds* [*retries*] [**periodic** | **on-demand**]	スイッチ 1 をスタンドアロン モードに変換します。 • *seconds* は、DPD メッセージの間隔（秒）を指定します。範囲は 10 ～ 3,600 秒です。 • *retries*（任意）は、DPD メッセージが失敗した場合に、DPD を再試行する間隔（秒）を指定します。範囲は 2 ～ 60 秒です。指定しない場合、デフォルトは 2 秒です。 • **periodic**（任意）は、DPD メッセージを定期的に送信することを指定します。 • **on-demand**（任意）は、DPD 再試行をオンデマンドで送信することを指定します。これがデフォルトの動作です。

（注）　**on-demand** オプションがデフォルトのため、**on-demand** キーワードはコンフィギュレーションの出力には表示されません。

DPD 設定の確認

DPD がイネーブルに設定されているかどうかを確認するには、グローバル モードで **show crypto isakmp sa detail** コマンドを入力します。

```
Router# show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Encr Hash Auth DH Lifetime Cap.
273   11.0.0.2        11.0.0.1        ivrf21   3des sha  psk  2  01:59:35 D
       Connection-id:Engine-id =  273:2(hardware)
```

Cisco IOS DPD に関する詳しい設定情報は、『*Cisco IOS Security Command Reference, Release 12.3*』を参照してください。

DPD の設定例は、「DPD の設定例」（P.27-24）を参照してください。

IPSec の NAT 透過の概要

IPSec NAT の透過機能は、Network Address Translation（NAT; ネットワーク アドレス変換）と IPSec の間にある多くの既知の問題を解決することにより、IP セキュリティ（IPSec）トラフィックがネットワーク上の NAT または Port Address Translation（PAT; ポート アドレス変換）ポイントを通過し、送受信できるようにします。

この機能が導入される前は、IPSec パケットの配信パス上に 1 つまたは複数の NAT または PAT ポイントが存在する場合、標準的な IPSec VPN トンネルは使用できませんでした。この機能を使用すると、IPSec が NAT/PAT デバイスを介して動作できます。

NAT 透過についての詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftipsnat.html

IPSec NAT の透過設定時の注意事項および制約事項

IPSec NAT 透過を設定する場合は、次の注意事項および制約事項に従ってください。

- IPSec 設定を介した非 GRE の場合、トンネル モードおよびトランスポート モードの両方で NAT 透過機能がサポートされます。
- IPSec 設定を介したポイントツーポイント GRE の場合、トンネル モードでのみ NAT 透過機能がサポートされます。
- DMVPN 構成の場合、トランスポート モードでのみ NAT 透過機能がサポートされます。

NAT 透過の設定

NAT 透過機能は、IPSec VPN SPA によって自動的に検出される機能です。設定作業は必要ありません。両方の VPN デバイスが NAT 透過機能対応であれば、NAT 透過機能は自動的に検出され、ネゴシエートされます。

NAT 透過機能のディセーブル化

ネットワークですでに IPSec 対応の NAT（spi-matching 方式）を使用している場合には、NAT 透過機能をディセーブルにできます。NAT 透過機能をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

```
Router(config)# no crypto ipsec nat-transparency udp-encapsulation
```

NAT キープアライブの設定

デフォルトでは、NAT キープアライブ機能はディセーブルです。NAT キープアライブ パケットを送信するようにルータを設定するには、グローバル コンフィギュレーション モードで **crypto isakmp nat keepalive** コマンドを入力します。

```
Router(config)# crypto isakmp nat keepalive seconds
```

このコマンドの *seconds* は、キープアライブ パケットの送信間隔（秒数）を指定します。範囲は 5 ～ 3,600 秒です。

NAT キープアライブの設定例は、「ISAKMP NAT 透過機能の設定例」（P.27-24）を参照してください。

NAT キープアライブ設定の確認

NAT の設定を確認するには、**show crypto ipsec sa** コマンドを入力します。

（注）　最初に **show crypto ipsec sa** コマンドを入力するときに、パケット カウンタでは正しい値が表示されない場合があります。更新された値を表示するコマンドを繰り返します。

```
Router# show crypto ipsec sa

interface:GigabitEthernet5/0/1
    Crypto map tag:testtag, local addr. 10.2.80.161

    local ident (addr/mask/prot/port):(10.2.80.161/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port):(100.0.0.1/255.255.255.255/0/0)
    current_peer:100.0.0.1:4500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps:109, #pkts encrypt:109, #pkts digest 109
    #pkts decaps:109, #pkts decrypt:109, #pkts verify 109
    #pkts compressed:0, #pkts decompressed:0
    #pkts not compressed:0, #pkts compr. failed:0, #pkts decompress failed:0
    #send errors 90, #recv errors 0

    local crypto endpt.:10.2.80.161, remote crypto endpt.:100.0.0.1:4500
    path mtu 1500, media mtu 1500
    current outbound spi:23945537

    inbound esp sas:
    spi:0xF423E273(4095992435)
    transform:esp-des esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    slot:0, conn id:200, flow_id:1, crypto map:testtag
    sa timing:remaining key lifetime (k/sec):(4607996/2546)
    IV size:8 bytes
    replay detection support:Y

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
    spi:0x23945537(596923703)
    transform:esp-des esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    slot:0, conn id:201, flow_id:2, crypto map:testtag
    sa timing:remaining key lifetime (k/sec):(4607998/2519)
    IV size:8 bytes
    replay detection support:Y

    outbound ah sas:

    outbound pcp sas:
```

Cisco IOS の IPSec NAT 透過機能のサポートに関する詳しい設定情報は、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftipsnat.html

設定例

ここでは、次の設定例を示します。

AES の設定例

この例では、Advanced Encryption Standard（AES; 高度暗号化規格）256 ビット キーをイネーブルに設定しています。

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
```

ISAKMP キーリングの設定例

以下に、ISAKMP プロファイルまたは ISAKMP キーリング設定の適用範囲を、ローカルの終端アドレスまたはインターフェイスに限定する例を示します。

ISAKMP プロファイルをローカル インターフェイスにバインドする設定例

以下に、ISAKMP プロファイルをローカル インターフェイスにバインドする例を示します。

```
crypto isakmp profile prof1
   keyring key0
   match identity address 11.0.0.2 255.255.255.255
   local-address serial2/0
```

ISAKMP キーリングをローカル インターフェイスにバインドする設定例

以下に、ISAKMP キーリングをインターフェイス serial2/0 だけにバインドする例を示します。

```
crypto keyring key0
  local-address serial2/0
  pre-shared-key address 11.0.0.2 key 12345
```

ISAKMP キーリングをローカル IP アドレスにバインドする設定例

以下に、ISAKMP キーリングを IP アドレス 10.0.0.2 だけにバインドする例を示します。

```
crypto keyring key0
  local-address 11.0.0.1
  pre-shared-key address 11.0.0.2 key 12345
```

証明書/ISAKMP プロファイル マッピングの設定例

以下に、証明書/ISAKMP プロファイル マッピングの設定例を示します。

- 「任意のフィールドに基づく証明書/ISAKMP プロファイル マッピングの設定例」（P.27-23）
- 「ISAKMP プロファイルに対応付けられたピアに割り当てられるグループ名の設定例」（P.27-23）

任意のフィールドに基づく証明書/ISAKMP プロファイル マッピングの設定例

以下に、証明書に「ou = green」が含まれる場合に、ISAKMP プロファイル「cert_pro」をピアに割り当てる例を示します。

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
```

ISAKMP プロファイルに対応付けられたピアに割り当てられるグループ名の設定例

以下に、ISAKMP プロファイルに割り当てられたピアに、グループ「some_group」を対応付ける例を示します。

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com

client configuration group some_group
```

暗号化事前共有キーの設定例

以下に、タイプ 6 の事前共有キーに暗号化を行った場合の設定例を示します。

```
Router(config)# password encryption aes
Router(config)# key config-key password-encrypt
New key:
Confirm key:
Router(config)#
0:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router(config)# exit
```

IKE の CAC の設定例

以下に、IKE の CAC を設定する例を示します。

- 「IKE SA 制限の設定例」（P.27-24）
- 「システム リソース制限の設定例」（P.27-24）

IKE SA 制限の設定例

以下に、IKE が新しい SA 要求を拒否するまでの SA の最大数を 25 に設定する例を示します。

```
Router(config)# crypto call admission limit ike sa 25
```

システム リソース制限の設定例

以下に、指定されたレベルのシステム リソースが使用されている場合に、IKE が SA 要求をドロップするように指定する例を示します。

```
Router(config)# call admission limit 50000
```

DPD の設定例

以下に DPD の設定例を示します。

- 「オンデマンド DPD の設定例」（P.27-24）
- 「定期的 DPD の設定例」（P.27-24）

オンデマンド DPD の設定例

以下に、オンデマンド DPD メッセージの設定例を示します。この例では、DPD メッセージは 60 秒おきに送信されます。ピアが応答しない場合は、5 秒おきに送信されます。

```
Router(config)# crypto isakmp keepalive 60 5
```

定期的 DPD の設定例

以下に、定期的 DPD メッセージの設定例を示します。この例では、DPD メッセージは 10 秒おきに送信されます。

```
Router(config)# crypto isakmp keepalive 10 periodic
```

ISAKMP NAT 透過機能の設定例

以下に、NAT キープアライブを 20 秒間隔で送信するための設定例を示します。

```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key 1234 address 56.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
!
```

```
crypto map test2 10 ipsec-isakmp
 set peer 56.0.0.1
 set transform-set t2
 match address 101
```