

IPsec

概要・基本設定	3
基本設定	3
ISAKMP/IKE による IPsec VPN	4
手動鍵による IPsec VPN	6
詳細設定	9
IPsec/ISAKMP モジュールの有効化	9
IPsec ポリシー (SPD)	9
SA 情報の設定	17
鍵管理の設定	20
その他	23
動作・設定の確認	28
基本的な情報	29
デバッグオプション	32
統計カウンター	33
コマンドリファレンス編	35
機能別コマンド索引	35
CREATE IPSEC BUNDLESPECIFICATION	37
CREATE IPSEC POLICY	39
CREATE IPSEC SASPECIFICATION	43
CREATE ISAKMP POLICY	45
DESTROY IPSEC BUNDLESPECIFICATION	49
DESTROY IPSEC POLICY	50
DESTROY IPSEC SASPECIFICATION	51
DESTROY ISAKMP POLICY	52
DISABLE IPSEC	53
DISABLE IPSEC POLICY DEBUG	54
DISABLE ISAKMP	56
DISABLE ISAKMP DEBUG	57
ENABLE IPSEC	58
ENABLE IPSEC POLICY DEBUG	59
ENABLE ISAKMP	62
ENABLE ISAKMP DEBUG	64
PURGE IPSEC	72
RESET IPSEC COUNTER	73

RESET IPSEC POLICY COUNTER	74
RESET IPSEC SA COUNTER	75
RESET ISAKMP COUNTER	76
SET IPSEC BUNDLESPECIFICATION	77
SET IPSEC POLICY	78
SET IPSEC SASPECIFICATION	81
SET IPSEC UDPPORT	83
SET ISAKMP POLICY	84
SHOW IPSEC	88
SHOW IPSEC BUNDLESPECIFICATION	89
SHOW IPSEC COUNTERS	91
SHOW IPSEC POLICY	96
SHOW IPSEC SA	104
SHOW IPSEC SASPECIFICATION	111
SHOW ISAKMP	114
SHOW ISAKMP COUNTERS	116
SHOW ISAKMP EXCHANGE	118
SHOW ISAKMP POLICY	122
SHOW ISAKMP SA	126

概要・基本設定

IPsec (IP security) は、IP に暗号化や認証などのセキュリティー機能を付加する一連のプロトコル群です。本製品は、暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着することにより IPsec を使用した安全性の高い VPN (Virtual Private Network) を構築できます。

※ 暗号・圧縮ボード (AR011) は AR700 シリーズでのみ使用できます。

※ IPsec は AR320 では使用できません。

IPsec を使用すると、次のようなことが可能になります。

- IP 通信の暗号化：IP を使うすべての通信 (WWW、FTP、Telnet など) を暗号化できます。IP 層で暗号化するため、上位の IP アプリケーションが IPsec に対応している必要はありません。また、暗号化をルーターで行うためユーザーが IPsec の存在を意識する必要がありません。
- IP 通信の改ざん検出：IP パケットに付加された認証データを検証することにより、通信経路上でのパケット改ざんを検出・防止できます。
- IP 通信の相手認証：IP パケットに付加された認証データを検証することにより、パケットの送信元が意図した相手であることを確認できます。
- IP 通信のトンネリング：ルーター間でパケットをトンネリングすることにより、プライベートネットワーク間の IP 通信が可能になります (VPN)。

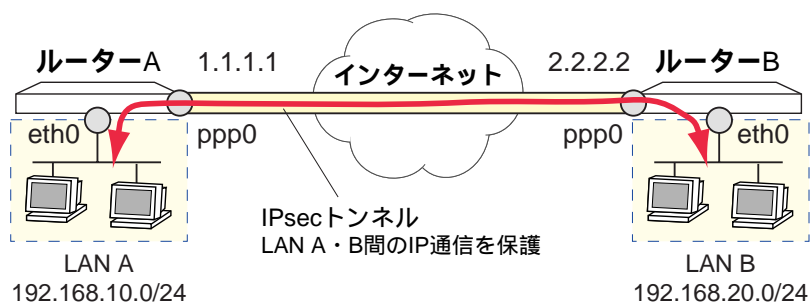
ここでは、本製品における IPsec の基本設定について解説します。

※ IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要があります。

基本設定

IPsec による VPN (以下、IPsec VPN) の基本構成を次に示します。本製品を使って IPsec VPN を構築するためには、最低限次の条件を満たす必要があります。

- 本製品 2 台に暗号ボードが装着されていること
- 本製品同士が IP で直接通信できること
- 少なくとも一方のルーターのアドレスが固定されていること



この構成の IPsec VPN では、次のような通信が可能です。

- プライベートネットワーク間の VPN 通信
 - トンネリングによるプライベート IP アドレスの隠蔽
 - IPsec による暗号化と認証データ付加
- インターネットとの（通常の）IP 通信

以下の各節では、上記の基本構成に基づき、IPsec の設定方法について解説します。

ISAKMP/IKE による IPsec VPN

ここでは、自動鍵管理による IPsec VPN 構築の要点を説明します。

ISAKMP/IKE を使用する場合は、以下の設定が必要です。

- IKE ネゴシエーションを行うための設定（ISAKMP ポリシー）
 - IPsec 通信の基本仕様の設定（SA スペックと SA バンドルスペック）
 - IPsec 通信の範囲指定（IPsec ポリシー）
1. IPsec VPN は、ルーター（セキュリティゲートウェイ）間で IP トンネルを張ることによって実現されます。そのためには、ルーター間で IP の通信ができなくてはなりません。各ルーターの接続形態に応じて、通常の IP 設定までをすませておいてください。
 2. 鍵管理プロトコル ISAKMP/IKE の設定を行います。最初に、ルーター間で認証を行うときに使う事前共有鍵（pre-shared key）を作成します。共有鍵なので、鍵の値は両方のルーターで同じでなくてはなりません。鍵番号は異なってもかまいません。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE="jogefoge" ↵
```

3. ISAKMP ポリシーを作成し、IKE ネゴシエーションの相手ルーターを登録します。PEER に相手ルーターの IP アドレスを、KEY に事前共有鍵の番号を指定してください。

```
CREATE ISAKMP POLICY=i PEER=2.2.2.2 KEY=1 SENDN=TRUE ↵
```

なお、相手ルーターのアドレスが不定な場合は PEER に ANY を指定し、代わりに相手ルーターの ID（任意の文字列）を「REMOTEID="RouterB"」のように指定してください。相手ルーター側では、自分の ID を「LOCALID="RouterB"」のように指定してください。

また、片側のアドレスが不定な場合は、「MODE=AGGRESSIVE」を指定して Aggressive モードを

使うようにしてください（省略時は Main モードになります）。

- アドレス固定側

```
CREATE ISAKMP POLICY=i PEER=ANY KEY=1 SENDN=TRUE
REMOTEID="RouterB" MODE=AGGRESSIVE ↵
```

- アドレス不定側

```
CREATE ISAKMP POLICY=i PEER=1.1.1.1 KEY=1 SENDN=TRUE
LOCALID="RouterB" MODE=AGGRESSIVE ↵
```

※ 両方のルーターのアドレスが不定な場合は、IPsec VPN を実用的に使用することはできません。通常の運用では、少なくとも片側のアドレスが固定になっている必要があります。

- 次に IPsec SA（IPsec の通信仕様）の設定を行います。SA スペックと SA バンドルスペックを作成し、IPsec 通信で使用するセキュリティプロトコルとアルゴリズムの組み合わせを指定します。ここでは、ESP（IP 暗号ペイロード）を使って IP パケットの暗号化と認証を行うための設定を示します。通常はこの設定で問題ないでしょう。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA ↵
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1" ↵
```

- ここから IPsec ポリシー（IPsec の適用範囲）の設定を行います。最初に ISAKMP メッセージ（始点・終点ともに UDP500 番）を素通しするためのポリシーを作成します。IPsec ポリシーの検索は作成順に行われるため、ISAKMP/IKE を使用する場合は必ず最初にこの設定を行ってください。INTERFACE パラメーターには、WAN 側インターフェースを指定します。その他は例のとおりで結構です。

```
CREATE IPSEC POLICY=isa INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
TRANSPORT=UDP ↵
```

- 次に IPsec を適用するパケットの条件（IPsec VPN のアドレス範囲）を指定します。IPsec VPN では、プライベート LAN 間の通信だけを IPsec の対象とします。少し長くなりますが、最低限以下のパラメーターを実際の環境に合わせて指定してください。

- INTERFACE：ルーターの WAN 側インターフェース
- BUNDLE：手順 4 で作成した SA バンドルスペックの番号
- PEER：相手ルーターの IP アドレス。相手のアドレスが不定なときは DYNAMIC を指定してください。
- LAD, LMA：ローカル側 LAN の範囲。LAD にネットワークアドレスを、LMA にネットマスクを指定します。
- RAD, RMA：リモート側 LAN の範囲。RAD にネットワークアドレスを、RMA にネットマスクを指定します。

```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=2.2.2.2 ↵
SET IPSEC POLICY=vpn LAD=192.168.10.0 LMA=255.255.255.0
  RAD=192.168.20.0 RMA=255.255.255.0 ↵
```

この例では、192.168.10.0/24 と 192.168.20.0/24 間の通信に IPsec を適用しています。

7. 最後に VPN 通信以外のパケットを素通しするポリシーを作成します。この設定は、インターネットへのアクセスが必要ない場合は省略してもかまいません。

```
CREATE IPSEC POLICY=inet INT=ppp0 ACTION=PERMIT ↵
```

＼ この構成では LAN 側のコンピューターにプライベートアドレスが設定されているため、実際に LAN からインターネットへアクセスするには NAT の設定が必要です。詳しくは「IPsec とファイアウォールの併用」をご覧ください。

8. IPsec と ISAKMP を有効にします。

```
ENABLE IPSEC ↵
ENABLE ISAKMP ↵
```

9. Security Officer レベルのユーザーを登録します。

```
ADD USER=secoff PASS=Passwords PRIVILEGE=SECURITYOFFICER ↵
```

10. Security Officer レベルのユーザーでログインしなおします。

```
LOGIN secoff ↵
```

11. 設定内容を保存し、次回起動時に読み込まれるように設定します。

```
CREATE CONFIG=ipsecvpn.cfg ↵
SET CONFIG=ipsecvpn.cfg ↵
```

12. セキュリティモードに移行します。

```
ENABLE SYSTEM SECURITY_MODE ↵
```

＼ Security Officer レベルのユーザーが登録されていないと、セキュリティモードに移行できません。

IPsec とファイアウォールや NAT を併用する場合は、追加の設定が必要になります。詳しくは「IPsec とファイアウォールの併用」をご覧ください。また、具体的な設定例については設定例集をご覧ください。

手動鍵による IPsec VPN

ここでは、手動鍵管理による IPsec VPN 構築の要点を説明します。

手動で鍵の管理を行う場合、以下の設定が必要です。

- IPsec 通信で使う暗号鍵・認証鍵の作成
- IPsec 通信の基本仕様の設定 (SA スペックと SA バンドルスペック)
- IPsec 通信の範囲指定 (IPsec ポリシー)

✎ 手動鍵を使う場合は、両方のルーターのアドレスが固定されていなくてはなりません。片側のアドレスが不定な場合は、ISAKMP/IKE による自動鍵管理をご使用ください。

1. IPsec VPN は、ルーター (セキュリティゲートウェイ) 間で IP トンネルを張ることによって実現されます。そのためには、ルーター間で IP の通信ができなくてはなりません。各ルーターの接続形態に応じて、通常の IP 設定までをすませておいてください。
2. IPsec 通信で使う暗号鍵と認証鍵を作成します。ここでは、暗号に 56 ビット DES を、認証に SHA-1 を使うものとします。これらの鍵は共有鍵なので、両方のルーターで同じになるように設定してください。ただし、鍵番号は異なってもかまいません。鍵作成の詳細については、「暗号・圧縮」の章をご覧ください。

通常は、片側のルーターでランダムに鍵を生成し、その値をもう一方のルーターに手動入力します。

```
CREATE ENCO KEY=1 TYPE=DES RANDOM DESCRIPTION="IPsec DES key" ↵
CREATE ENCO KEY=2 TYPE=GENERAL LENGTH=20 RANDOM DESCRIPTION="IPsec
SHA-1 key" ↵
```

作成した鍵の値を表示させるには、SHOW ENCO KEY コマンド (「暗号・圧縮」の 49 ページ) を使います。

```
Manager > show enco key=1

          9cemvrwgn5hvek
          0xF888CAC6C66ECF52

Manager > show enco key=2

0x431d62cd3cb76fb8101dacaf43aa4dbfb919e957
```

もう一方のルーターに手動で鍵の値を入力します。

```
CREATE ENCO KEY=1 TYPE=DES VALUE=0xF888CAC6C66ECF52
DESCRIPTION="IPsec DES key" ↵
CREATE ENCO KEY=2 TYPE=GENERAL
VALUE=0x431d62cd3cb76fb8101dacaf43aa4dbfb919e957 DESCRIPTION="IPsec
SHA-1 key" ↵
```

3. 次に IPsec SA (IPsec の通信仕様) の設定を行います。SA スペックと SA バンドルスペックを作成し、IPsec 通信で使用するセキュリティプロトコルとアルゴリズムの組み合わせ、暗号鍵と認証鍵、外向き・内向きの SPI 値 (256 ~ 4294967295) を指定します。ここでは、ESP (IP 暗号ペイロード)

を使って IP パケットの暗号化と認証を行うための設定を示します。通常はこの設定で問題ないでしょう。相手ルーターでは、INSPI と OUTSPI の値を入れ替えてください。

```
CREATE IPSEC SASPEC=1 KEYMAN=MANUAL PROT=ESP ENCALG=DES ENCKEY=1
    HASHALG=SHA HASHKEY=2 INSPI=1000 OUTSPI=1001 ↵
CREATE IPSEC BUNDLE=1 KEYMAN=MANUAL STRING="1" ↵
```

4. ここから IPsec ポリシー（IPsec の適用範囲）の設定を行います。最初に IPsec を適用するパケットの条件（IPsec VPN のアドレス範囲）を指定します。IPsec VPN では、プライベート LAN 間の通信だけを IPsec の対象とします。少し長くなりますが、最低限以下のパラメーターを実際の環境に合わせて指定してください。

- INTERFACE：ルーターの WAN 側インターフェース
- BUNDLE：手順 4 で作成した SA バンドルスペックの番号
- PEER：相手ルーターの IP アドレス。相手のアドレスが不定なときは手動鍵は使用できません。
- LAD, LMA：ローカル側 LAN の範囲。LAD にネットワークアドレスを、LMA にネットマスクを指定します。
- RAD, RMA：リモート側 LAN の範囲。RAD にネットワークアドレスを、RMA にネットマスクを指定します。

```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=MANUAL BUNDLE=1
    PEER=2.2.2.2 ↵
SET IPSEC POLICY=vpn LAD=192.168.10.0 LMA=255.255.255.0
    RAD=192.168.20.0 RMA=255.255.255.0 ↵
```

この例では、192.168.10.0/24 と 192.168.20.0/24 間の通信に IPsec を適用しています。

5. 最後に VPN 通信以外のパケットを素通しするポリシーを作成します。この設定は、インターネットへのアクセスが必要ない場合は省略してもかまいません。

```
CREATE IPSEC POLICY=inet INT=ppp0 ACTION=PERMIT ↵
```

※ この構成では LAN 側のコンピューターにプライベートアドレスが設定されているため、実際に LAN からインターネットへアクセスするには NAT の設定が必要です。詳しくは「IPsec とファイアウォールの併用」をご覧ください。

6. IPsec を有効にします。

```
ENABLE IPSEC ↵
```

7. Security Officer レベルのユーザーを登録します。

```
ADD USER=secoff PASS=PasswordS PRIVILEGE=SECURITYOFFICER ↵
```

8. Security Officer レベルのユーザーでログインしなおします。

```
LOGIN secoff ↵
```


9. 設定内容を保存し、次回起動時に読み込まれるように設定します。

```
CREATE CONFIG=ipsecvpn.cfg ↵
SET CONFIG=ipsecvpn.cfg ↵
```

10. セキュリティーモードに移行します。

```
ENABLE SYSTEM SECURITY_MODE ↵
```

※ Security Officer レベルのユーザーが登録されていないと、セキュリティーモードに移行できません。

IPsec とファイアウォールや NAT を併用する場合は、追加の設定が必要になります。詳しくは「IPsec とファイアウォールの併用」をご覧ください。また、具体的な設定例については設定例集をご覧ください。

詳細設定

IPsec に関する各種設定の詳細について解説します。個々のパラメーターについては、コマンドリファレンスをご覧ください。

IPsec/ISAKMP モジュールの有効化

IPsec を使用するためには、ENABLE IPSEC コマンド (58 ページ) で IPsec モジュールを有効にする必要があります。

```
ENABLE IPSEC ↵
```

自動鍵管理 (ISAKMP/IKE) を使う場合は、ENABLE ISAKMP コマンド (62 ページ) で ISAKMP モジュールも有効にします。

```
ENABLE ISAKMP ↵
```

IPsec の有効・無効は、SHOW IPSEC コマンド (88 ページ) で確認できます。

```
SHOW IPSEC ↵
```

ISAKMP の有効・無効は、SHOW ISAKMP コマンド (114 ページ) で確認できます。

```
SHOW ISAKMP ↵
```

IPsec ポリシー (SPD)

セキュリティーポリシーデータベース (SPD) は、パケットにどのような処理を行うかを定義するデータベースです。始点・終点アドレスやプロトコル、ポート番号をもとにパケットを識別し、該当する処理を実行します。IPsec におけるパケットフィルターと考えてもよいでしょう。

SPD は個々の IPsec ポリシーによって構成されます。IPsec ポリシーの作成は、CREATE IPSEC POLICY

コマンド（39 ページ）で行います。

IPsec ポリシーは、最小限以下の要素で構成されます。

```
CREATE IPSEC POLICY=name INTERFACE=interface ACTION={DENY|IPSEC|PERMIT}
  selectors... ipsec_params... ↵
```

パラメーター	説明
POLICY	ポリシー名。任意です
INTERFACE	適用インターフェース。IPsec ポリシーはインターフェースごとに設定します。ポリシーの検索は、パケットが指定インターフェースから送信されるとき、および、指定インターフェースで受信したときに行われます。通常は WAN 側のインターフェースを指定します
ACTION	パケットに対する処理（アクション）。IPsec 適用、通過、拒否の 3 種類があります（別表参照）。ポリシーの順番に気を付けてください
selectors...	パケットの条件指定パラメーター。始点・終点アドレス、プロトコル、ポートなど、パケットを分類するための条件を指定します（別表参照）
ipsec_params...	IPsec 処理に関するパラメーター。アクションとして「IPsec 適用」を選択したときだけ指定します（別表参照）

表 1: IPsec ポリシーの基本パラメーター

パケットの条件指定（selectors...）には、以下のパラメーターを使います。ここでの「ローカル側」とは、送信パケットでは始点、受信パケットでは終点のことを意味します。また「リモート側」も同様で、送信パケットでは終点、受信パケットでは始点のことになります。IPsec ではこれらのフィルタリング条件を「セレクター」と呼んでいます。

パラメーター	説明
LADDRESS	ローカル側 IP アドレス
LMASK	LADDRESS に対するネットマスク
LNAME	ローカル側システム名（フェーズ 2 ID）
LPORT	ローカル側ポート番号（プロトコルが TCP か UDP のときのみ）
RADDRESS	リモート側 IP アドレス
RMASK	RADDRESS に対するネットマスク
RNAME	リモート側システム名（フェーズ 2 ID）
RPORT	リモート側ポート番号（プロトコルが TCP か UDP のときのみ）
TRANSPORTPROTOCOL	IP プロトコルタイプ（TCP、UDP など）

表 2: IPsec ポリシーの条件パラメーター

また、マッチしたパケットに対する処理は ACTION パラメーターで指定します。

アクション	説明
-------	----

PERMIT	パケットを通過させる (IPsec を適用しない)
IPSEC	パケットに IPsec 処理を適用する (BUNDLESPECIFICATION パラメーターで指定した SA バンドルの処理を適用する)
DENY	パケットを破棄する

表 3: IPsec ポリシーのアクション

IPsec 処理を指定した場合 (ACTION=IPSEC) は、さらに以下の IPsec 関連パラメーター (ipsec_params...) も指定します。

パラメーター	説明
BUNDLESPECIFICATION	SA バンドルスペック。IPsec 処理 (SA スペックで記述) の組み合わせを記述した SA バンドルスペックの番号を指定します
KEYMANAGEMENT	鍵管理方式。鍵を自動 (ISAKMP) で管理するか手動 (MANUAL) で管理するかを指定します
PEERADDRESS	対向 IPsec 機器のアドレス。トンネルモード SA の場合は、カプセル化したパケットの送り先 (トンネルの終端) を指定します。また、トランスポートモード SA の場合は、対象パケットの最終的な送信先を指定します

表 4: IPsec 関連パラメーター

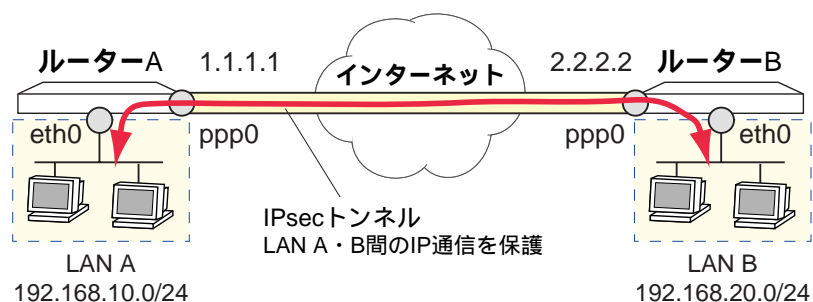
以下、具体例を示します。IPsec ポリシーの設定コマンドは長くなりがちなので、CREATE と SET に分けています。また、適宜省略形をご使用ください。

ISAKMP パケット (始点・終点とも UDP500 番) を通過させるポリシー「isa」を作成します。ISAKMP/IKE を使うときは、必ずこのポリシーを作成してください。そのとき、IPsec を適用するポリシー (ACTION=IPSEC) よりも前にこのポリシーを置いてください。

```
CREATE IPSEC POLICY=isa INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
TRANSPORT=UDP ↵
```

このコマンドは、「ppp0 から送出する IP パケットのうち、始点・終点ポートが 500 番の UDP パケットは IPsec を適用せずにそのまま送信する。また、ppp0 で受信したパケットのうち、始点・終点ポートが 500 番の UDP パケットには IPsec の復号化処理を適用せずにそのまま受け入れる」の意味になります。

ローカル側 LAN (192.168.10.0/24) とリモート側 LAN (192.168.20.0/24) の間の通信に IPsec 処理を適用するポリシー「vpn」を作成します。IPsec 処理の内容は BUNDLESPECIFICATION パラメーターで指定した SA バンドルスペックによって定義します (詳細は「SA 情報の設定」をご覧ください)。トンネルモード用のポリシー例です。また、IPsec 処理後のパケットの送り先は PEERADDRESS パラメーターで指定します。ここでは自動鍵を使っています。



```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=2.2.2.2 ↵
SET IPSEC POLICY=vpn LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.20.0
    RMA=255.255.255.0 ↵
```

このコマンドは、「ppp0 から送出する IP パケットのうち、始点アドレスが 192.168.10.0/24 (192.168.10.0 ~ 192.168.10.255) の範囲で、終点アドレスが 192.168.20.0/24 (192.168.20.0 ~ 192.168.20.255) の範囲のものに対し、バンドルスベック「1」の IPsec 処理を施した上でパケットに新しい IP (トンネル) ヘッダーを付け、対向 IPsec 機器 2.2.2.2 に送信する。また、ppp0 で受信した IPsec パケットのうち、バンドルスベック「1」の処理内容と合致しているものに対して復号化処理を行い、復号化後のパケットの始点アドレスが 192.168.20.0/24 の範囲で、終点アドレスが 192.168.10.0/24 の範囲であれば受け入れる」の意味になります。

＼ 手動鍵の場合は、KEYMANAGEMENT パラメーターに MANUAL を指定してください。

相手ルーターのアドレスが不定なときは PEERADDRESS に DYNAMIC を指定します。これは、ISAKMP の認証をパスした相手のアドレスを意味します。このようなケースでは、常にアドレス不定側から通信が開始されることになります。

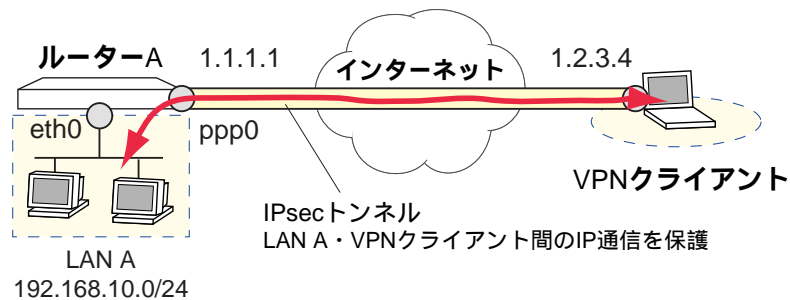
```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=DYNAMIC ↵
SET IPSEC POLICY=vpn LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.20.0
    RMA=255.255.255.0 ↵
```

このとき、相手ルーター (アドレス不定側) の対応するポリシーは次のようになります。アドレス不定側では相手ルーターのアドレスがわかっているので、PEERADDRESS には固定アドレスが入ります。

```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=1.1.1.1 ↵
SET IPSEC POLICY=vpn LAD=192.168.20.0 LMA=255.255.255.0 RAD=192.168.10.0
  RMA=255.255.255.0 ↵
```

※ 片側のアドレスが不定なときは ISAKMP/IKE (Aggressive モードまたは XAUTH) を使ってください。アドレスが不定なときは手動鍵は使えません。

ローカル側 LAN (192.168.10.0/24) と VPN クライアント (1.2.3.4) の間の通信に IPsec 処理を適用するポリシー「vpncli」を作成します。PEERADDRESS と RADDRESS が同じになっていることと、リモート側アドレス (RADDRESS、RMASK) がホストアドレスになっている点に注目してください (RMASK 省略時はホストマスク 255.255.255.255 となります)。



```
CREATE IPSEC POLICY=vpncli INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=1.2.3.4 ↵
SET IPSEC POLICY=vpncli LAD=192.168.10.0 LMA=255.255.255.0 RAD=1.2.3.4 ↵
```

VPN クライアントのアドレスが不定なときは PEERADDRESS に DYNAMIC を指定します。これは、ISAKMP の認証をパスした相手のアドレスを意味します。また、パケット条件のリモート側アドレスも不定になるため、RADDRESS の代わりに RNAME (相手のフェーズ 2 ID) を使います。このようなケースでは、常にアドレス不定側から通信が開始されることになります。

```
CREATE IPSEC POLICY=vpncli INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=DYNAMIC ↵
SET IPSEC POLICY=vpncli LAD=192.168.10.0 LMA=255.255.255.0
  RNAME=clientname ↵
```

このとき、VPN クライアント側の対応するポリシーは次のようになります。クライアント側では相手ルーターのアドレスがわかっているので、PEERADDRESS には固定アドレスが入ります。ただし、自分のアドレスが不定なので LADDRESS の代わりに LNAME (自分のフェーズ 2 ID) を使います。

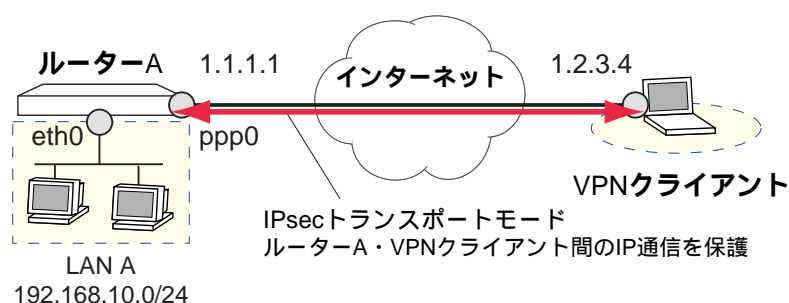
```
CREATE IPSEC POLICY=vpncli INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=1.1.1.1 ↵
SET IPSEC POLICY=vpncli LNAME=clientname RAD=192.168.10.0
  RMA=255.255.255.0 ↵
```

※ 片側のアドレスが不定なときは ISAKMP/IKE (Aggressive モードまたは XAUTH) を使ってください。アドレスが不定なときは手動鍵は使えません。

複数の VPN クライアントと通信するときは、クライアントごとに IPsec ポリシーを作成する必要があります。クライアントのアドレスが不定な場合は、クライアントごとに異なる LNAME、RNAME を設定してください。次の例では、3 つのクライアント (client1、client2、client3) との接続を想定しています。IPsec 処理の内容は全クライアント共通と仮定しているため、BUNDLE には同じバンドルスペックを指定しています。クライアント側の設定でも、それぞれ対応する LNAME を指定してください。

```
CREATE IPSEC POLICY=v1 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=DYNAMIC ↵
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=client1 ↵
CREATE IPSEC POLICY=v2 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=DYNAMIC ↵
SET IPSEC POLICY=v2 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=client2 ↵
CREATE IPSEC POLICY=v3 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=DYNAMIC ↵
SET IPSEC POLICY=v3 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=client3 ↵
```

トランスポートモードの場合は、パケット条件のローカル側アドレス (LADDRESS) が自分のアドレスと同じになり、リモート側アドレス (RADDRESS) が対向 IPsec 機器アドレス (PEERADDRESS) と同じになります。この設定では、ルーター A と VPN クライアント間の IP 通信だけが保護の対象となります (VPN クライアントから LAN A にはアクセスできません)。

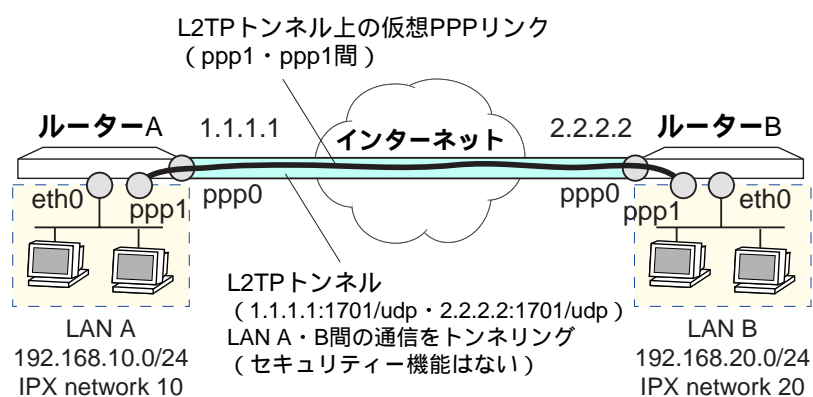


```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=2
    PEER=1.2.3.4 ↵
SET IPSEC POLICY=vpn LAD=1.1.1.1 RAD=1.2.3.4 ↵
```

このコマンドは、「ppp0 から送出する IP パケットのうち、始点アドレスが 1.1.1.1 で終点アドレスが 1.2.3.4 のものに対し、バンドルスペック「2」の IPsec 処理を施した上で対向 IPsec 機器 1.2.3.4 に送信する。また、ppp0 で受信した IPsec パケットのうち、バンドルスペック「2」の処理内容と合致しているものに対して復号化処理を行い、復号化後のパケットの始点アドレスが 1.2.3.4 で終点アドレスが 1.1.1.1 であれば受け入れる」の意味になります。

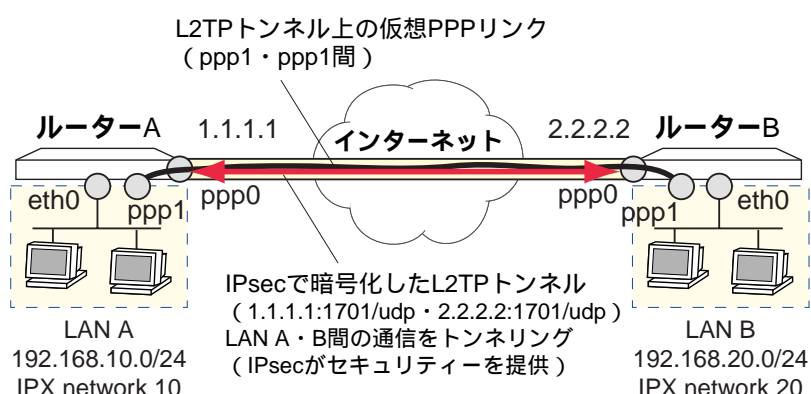
＼ SA スペック、バンドルスペックの設定については「SA 情報の設定」をご覧ください。

本製品でトランスポートモードを使うケースはまれですが、L2TP と併用するときにはトランスポートモードが有効に働きます。例として次のような L2TP VPN を考えます。



この構成ではルーター A・B 間に L2TP のトンネルを張って、LAN A・B 間の通信 (IP と IPX) をトンネリングしています。L2TP は PPP をトンネリングするため複数のプロトコルを通すことができますが、暗号化・認証などのセキュリティ機能はありません。L2TP トンネルにセキュリティを付加するには、トランスポートモードの IPsec を併用します。

L2TP トンネルの実体は、ルーター A・B 間の UDP パケット (始点・終点ともに 1701 番) です。これは 1 対 1 の通信なので、このパケットにトランスポートモードの IPsec を適用すれば L2TP トンネルを暗号化できることになります。



```
CREATE IPSEC POLICY=l2 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=3
  PEER=2.2.2.2 ↵
SET IPSEC POLICY=vpn LAD=1.1.1.1 LPORT=1701 RAD=2.2.2.2 RPORT=1701
  TRANSPORT=UDP ↵
```

このコマンドは、「ppp0 から送出する IP パケットのうち、始点アドレス 1.1.1.1、始点ポート 1701、終点アドレス 2.2.2.2、終点ポート 1701 の UDP パケットに対し、バンドルスペック「3」の IPsec 処理を施した上で対向 IPsec 機器 2.2.2.2 に送信する。また、ppp0 で受信した IPsec パケットのうち、バンドルスペック「3」の処理内容と合致しているものに対して復号化処理を行い、復号化後のパケットの始点アドレスが 2.2.2.2、始点ポートが 1701、終点アドレスが 1.1.1.1、終点ポートが 1701、プロトコルが UDP であれば受け入れる」の意味になります。

すべてのパケットを通過させるポリシー「inet」を作成します。IPsec 適用範囲外のパケットに対して通常の通信を許可する場合は、最後にこのポリシーを作成してください。インターフェースに対して 1 つでも IPsec ポリシーを作成すると、ポリシーリストの末尾にすべてのパケットを破棄する暗黙のポリシーが作成されます。そのため、下記のポリシーを作成しない場合は、IPsec 通信の範囲外ではまったく通信ができません。この例のようにパケット条件パラメーターを指定しない場合は「すべてのパケット」を意味します。

```
CREATE IPSEC POLICY=inet INT=ppp0 ACTION=PERMIT ↵
```

SPD のチェックは、ポリシーが設定されているインターフェース上でパケットを送受信するときに行われます。このとき、データベース内の各ポリシーが作成した順に検索され、最初に一致したポリシーで指定された処理が行われます。そのため、ポリシーの順序には十分留意してください。また、ポリシーリストの末尾にはすべてのパケットを破棄 (DENY) する暗黙のポリシーが存在するため、IPsec を適用しない通信を許可するときは、最後にすべてのパケットを通過させる (PERMIT) ポリシーを作成してください。

SPD (ポリシーの一覧) は SHOW IPSEC POLICY コマンド (96 ページ) で表示できます。

```
SHOW IPSEC POLICY ↵
```

各ポリシーの詳細を確認するには、POLICY パラメーターにポリシー名を指定します。


```
SHOW IPSEC POLICY=vpn ↵
```

SA 情報の設定

パケットに適用する IPsec 処理の詳細は、SA スペックとバンドルスペックで定義します。

SA スペック

SA スペックでは適用するプロトコル、アルゴリズム、鍵管理方式、SA モードを指定し、手動鍵の場合はさらに鍵と SPI も指定します。SA スペックは CREATE IPSEC SASPECIFICATION コマンド（43 ページ）で定義します。1 つの SA スペックでは、プロトコルやアルゴリズムを 1 つしか指定できません。複数のプロトコルを組み合わせ使いたいときは、後述するバンドルスペックで組み合わせを指定します（使用プロトコルが 1 つしかないときでもバンドルスペックは必要です）。

```
CREATE IPSEC SASPECIFICATION=spec-id KEYMANAGEMENT={ISAKMP|MANUAL}
  PROTOCOL={AH|COMP|ESP} [MODE={TRANSPORT|TUNNEL}] algorithms... keys...
  spis... ↵
```

以下、具体例を示します。

自動鍵で ESP トンネルモードによる暗号化と認証を行う SA スペック「1」を作成します。ESP を使うときは、暗号アルゴリズム（ENCALG）と認証アルゴリズム（HASHALG）を指定してください。MODE パラメーター省略時はトンネルモードになります。鍵と SPI は ISAKMP/IKE によって自動的にネゴシエーションされます。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTO=ESP ENCALG=DES HASHALG=SHA ↵
```

ESP では暗号化と認証の両機能を使用できますが、アルゴリズムに NULL を指定すると、どちらか一方だけを使うよう設定することもできます。たとえば、DES による暗号化だけを行い、認証機能を使わない場合は次のようにします。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTO=ESP ENCALG=DES HASHALG=NULL ↵
```

また、暗号化を行わず（NULL 暗号化）に認証機能だけを使う場合は次のようにします。これは、ESP のデバッグに便利です。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTO=ESP ENCALG=NULL HASHALG=SHA ↵
```

※ ENCALG と HASHALG の両方に NULL を指定することはできません。

手動鍵で ESP トンネルモードによる暗号化と認証を行う SA スペック「1」を作成します。手動鍵の場合は、暗号鍵（ENCKEY）、認証鍵（HASHKEY）と送信時 SPI（OUTSPI）、受信時 SPI（INSPI）を手動で設定する必要があります。INSPI と OUTSPI は、対向 IPsec 機器と逆になるように設定してください。

```
CREATE IPSEC SASPEC=1 KEYMAN=MANUAL PROTO=ESP ENCALG=DES HASHALG=SHA
  ENCKEY=1 HASHKEY=2 INSPI=1000 OUTSPI=1001 ↵
```

自動鍵で AH トンネルモードによる認証を行う SA スペック「2」を作成します。AH を使うときは、認証アルゴリズム (HASHALG) を指定してください。MODE パラメーター省略時はトンネルモードになります。鍵と SPI は ISAKMP/IKE によって自動的にネゴシエーションされます。

```
CREATE IPSEC SASPEC=2 KEYMAN=ISAKMP PROTO=AH HASHALG=SHA ↵
```

手動鍵で AH トンネルモードによる認証を行う SA スペック「2」を作成します。手動鍵の場合は、認証鍵 (HASHKEY) と送信時 SPI (OUTSPI)、受信時 SPI (INSPI) を手動で設定する必要があります。INSPI と OUTSPI は、対向 IPsec 機器と逆になるように設定してください。

```
CREATE IPSEC SASPEC=2 KEYMAN=MANUAL PROTO=AH HASHALG=SHA HASHKEY=2
  INSPI=2000 OUTSPI=2001 ↵
```

自動鍵で IPComp によるペイロード圧縮を行う SA スペック「3」を作成します。IPComp を使うときは、圧縮アルゴリズム「LZS」だけを指定してください。

```
CREATE IPSEC SASPEC=3 KEYMAN=ISAKMP PROTO=COMP COMPALG=LZS ↵
```

- ＼ IPComp を使うときは、圧縮用のソフトウェアチャンネルを接続先拠点数にかかわらず 1 チャンネル確保してください。これには SET ENCO SW コマンド(「暗号・圧縮」の 35 ページ)の STACCHANNELS パラメーターを使います。チャンネル確保の設定はルーターを再起動しないと有効になりませんのでご注意ください。なお、暗号・圧縮ボードを装着している場合は本コマンドは必要ありません(実行するとメモリーの無駄になります)。

```
SET ENCO SW STACCHANNELS=1 ↵
```

手動鍵で IPComp によるペイロード圧縮を行う SA スペック「3」を作成します。

```
CREATE IPSEC SASPEC=3 KEYMAN=MANUAL PROTO=COMP COMPALG=LZS ↵
```

SA スペックの設定内容は、SHOW IPSEC SASPECIFICATION コマンド(111 ページ)で確認できます。

```
SHOW IPSEC SASPECIFICATION ↵
SHOW IPSEC SASPECIFICATION=1 ↵
```

SA スペックに基づいて確立された SA の情報は SHOW IPSEC SA コマンド(104 ページ)で確認できます。

```
SHOW IPSEC SA ↵
SHOW IPSEC SA=1 ↵
```

バンドルスペック

バンドルスペックでは、プロトコルごとに定義した SA スペックの組み合わせを指定します。バンドルは、パケットに対して複数のプロトコルを適用するためのメカニズムですが、プロトコルを 1 つしか使わないときであってもバンドルスペックを定義する必要があります。IPsec ポリシーのアクションで「ACTION=IPSEC」を指定するときに、処理内容をバンドルスペックの番号で指定するためです。

バンドルスペックは CREATE IPSEC BUNDLESPECIFICATION コマンド (37 ページ) で作成します。

```
CREATE IPSEC BUNDLESPECIFICATION=bspec-id KEYMANAGEMENT={ISAKMP|MANUAL} ㊟
STRING="bundle-string" sa_lifetime... ㊟
```

最低限、バンドルスペック番号、鍵管理方式、SA スペックの組み合わせを指定してください。

SA スペックの組み合わせは STRING パラメーターで指定します。このパラメーターを指定するときは、3 種類の記号「AND」、「OR」、「,」を使うことができます。以下、それぞれの使い方を示します。ここでは、説明のため次のような SA スペックが定義されているものと仮定します。

番号	プロトコル	暗号方式	認証方式	圧縮方式
1	ESP	DES	SHA1	-
2	ESP	DES	MD5	-
3	AH	-	SHA1	-
4	AH	-	MD5	-
5	IPComp	-	-	STAC LZS

表 5: SA スペックのサンプル

プロトコルを 1 つしか適用しない場合は、使用する SA スペックの番号を 1 つだけ指定します。たとえば、ESP (DES + SHA1) を適用するときは STRING パラメーターに次のように指定します。

```
"1" ㊟
```

「AND」は、併用するプロトコルの組み合わせと適用順序を示します。「AND」でつなげる SA スペックはそれぞれ異なるプロトコルでなくてはなりません。たとえば、IPComp (LZS)、ESP (DES + SHA1)、AH (SHA1) の順に適用する場合は、次のように指定します。

```
"5 and 1 and 3" ㊟
```

プロトコルの適用順序は、通常 IPComp、ESP、AH の順とします。IPComp は必ず最初に適用しなくてはなりません。

ISAKMP/IKE を使用する場合は、プロトコルの組み合わせもネゴシエーションによって決定されます。そのため、バンドルスペックでは可能な組み合わせ (候補) を複数記述できます。「OR」と「,」はそのための記号です (手動鍵のときは使えません)。

「OR」は、使用するアルゴリズムの選択肢を示すもので、同一プロトコルでアルゴリズムが異なる SA スペックを指定します。たとえば、IPComp、ESP、AH の順にプロトコル適用する場合で、AH の認証アルゴリズムとして SHA1 か MD5 のどちらか一方を使いたい場合は、次のように指定します。

```
"5 and 1 and 3 or 4" ↵
```

「,」(カンマ)は、組み合わせパターンを複数提示したいときに使います。「IPComp (LZS) \ ESP (DES + SHA1) \ AH (SHA1)」の組み合わせが第1候補、「ESP (DES + SHA1) \ AH (SHA1)」が第2候補、「ESP (DES + SHA1)」のみが第3候補なら次のように指定します。

```
"5 and 1 and 3, 1 and 3, 1" ↵
```

以下、バンドルスペックの作成例を示します。SA スペックは先ほどの例をもとにします。

自動鍵で ESP (DES + SHA1) を使うバンドルスペック「1」を作成します。

```
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STR="1" ↵
```

手動鍵で ESP (DES + MD5) \ AH (MD5) の順に適用するバンドルスペック「2」を作成します。

```
CREATE IPSEC BUNDLE=2 KEYMAN=MANUAL STR="2 and 4" ↵
```

自動鍵で「IPComp (LZS) \ ESP (DES + SHA1)」を第1候補、「ESP (DES + SHA1)」のみを第2候補とするバンドルスペック「3」を作成します。

```
CREATE IPSEC BUNDLE=3 KEYMAN=ISAKMP STR="5 and 1, 1" ↵
```

バンドルスペックの設定内容は、SHOW IPSEC BUNDLESPECIFICATION コマンド (89 ページ) で確認できます。

```
SHOW IPSEC BUNDLESPECIFICATION ↵
SHOW IPSEC BUNDLESPECIFICATION=1 ↵
```

実際に確立された SA バンドルの情報は、SHOW IPSEC POLICY コマンド (96 ページ) の SABUNDLE オプションで確認できます。

```
SHOW IPSEC POLICY SABUNDLE ↵
SHOW IPSEC POLICY=v1 SABUNDLE ↵
```

鍵管理の設定

ISAKMP/IKE による自動鍵管理

自動鍵管理の設定は ISAKMP ポリシーによって行います。ISAKMP ポリシーは、フェーズ 1 で ISAKMP SA を確立するためのパラメーターを定義するもので、相手機器のアドレスや認証方式、ISAKMP SA 上で使用するアルゴリズムなどについて設定します。

ISAKMP ポリシーを定義しておけば、IPsec 処理の必要なパケットが検出されたときに、適切な相手機器

との間で自動的にネゴシエーションが開始されます。まだフェーズ 1 が開始されていないときは、最初に ISAKMP SA を確立し、その後フェーズ 2 で ISAKMP SA の保護を受けながら IPsec SA のネゴシエーションを行います。

フェーズ 1 のネゴシエーションにおける相手認証の方式としては、共有パスフレーズによる事前共有鍵 (pre-shared key) 方式と RSA デジタル署名方式を使用できます。デフォルトは事前共有鍵方式です。

- ✧ RSA デジタル署名方式では PKI モジュールを使用するため、別売の PKI フィーチャーライセンス (AT-FL-06) が必要です。

ISAKMP ポリシーは CREATE ISAKMP POLICY コマンド (45 ページ) で作成します。事前共有鍵方式で相手認証を行う場合、最低限必要なパラメーターは次のとおりです。ポリシー名、相手機器のアドレス、事前共有鍵の番号を指定してください。「SENDNOTIFY=TRUE」は相互接続性のためのパラメーターです。

```
CREATE ISAKMP POLICY=name PEER={ipadd|ANY} [KEY=0..65535]
SENDNOTIFY=TRUE ↵
```

事前共有鍵は CREATE ENCO KEY コマンド (「暗号・圧縮」の 18 ページ) で作成する汎用鍵 (TYPE=GENERAL) です。次のようにして作成してください。鍵の作成方法の詳細については「暗号・圧縮」の章をご覧ください。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE="pobaetrpnjkakdf" ↵
```

以下、事前共有鍵方式を使う場合の ISAKMP ポリシーの作成例を示します。

「2.2.2.2」との間で ISAKMP/IKE のネゴシエーションを行う ISAKMP ポリシー「i」を作成します。事前共有鍵の番号は「1」とします。

```
CREATE ISAKMP POLICY=i PEER=2.2.2.2 KEY=1 SENDN=TRUE ↵
```

このコマンドは、「2.2.2.2 とのネゴシエーションでは事前共有鍵「1」を用いる」の意味になります。

相手機器のアドレスが不定なときは PEER に ANY を指定します。これは、どのアドレスからのネゴシエーション要求であっても受け入れることを示します。しかし、これでは相手の識別ができないため、アドレス不定側で ID ペイロードの内容を明示的に指定することで相手を識別します。

このように、片側のアドレスが不定で ID 認証を行う場合は、デフォルトの Main モードではなく、Aggressive モードを使う必要があります。また、このようなケースでは、ISAKMP ネゴシエーションは常にアドレス不定側から開始されることになります。

アドレス固定側では、REMOTEID パラメーターで相手の ID を指定します。相手から受け取った ID ペイロードの中身が REMOTEID で指定した値と一致しており、なおかつ、事前共有鍵の値が一致していれば認証成功となります。

```
CREATE ISAKMP POLICY=i PEER=ANY KEY=1 REMOTEID=client MODE=AGGRESSIVE
SENDN=TRUE ↵
```

このコマンドは、「ID 値が client である相手とのネゴシエーションでは事前共有鍵「1」を用いる」の意味になります。

また、アドレス不定側では、LOCALID パラメーターで自分の ID を明示的に指定します。

```
CREATE ISAKMP POLICY=i PEER=1.1.1.1 KEY=1 LOCALID=client MODE=AGGRESSIVE
SENDN=TRUE ↵
```

＼ LOCALID を指定しなかった場合、ID ペイロードには自分の IP アドレスがセットされます。

複数の相手と接続する場合は、通信相手の数だけ ISAKMP ポリシーを作成し、それぞれ個別に事前共有鍵を指定します。相手のアドレスが固定ならば、次のようにします。ここでは、2.2.2.2 と 3.3.3.3 との接続を想定しています。2.2.2.2 とのネゴシエーションでは事前共有鍵「1」を、3.3.3.3 とは「2」を使って認証を行います。

```
CREATE ISAKMP POLICY=two PEER=2.2.2.2 KEY=1 SENDN=TRUE ↵
CREATE ISAKMP POLICY=three PEER=3.3.3.3 KEY=2 SENDN=TRUE ↵
```

複数の相手と接続する場合で相手のアドレスが不定の場合は、次のようにします。IP アドレスでは相手を識別できないため、相手が送ってくる ID ペイロードの値を一種のユーザー名（あるいはホスト名）として利用します。このように片側のアドレスが不定なときは Aggressive モードが必須です。ここでは、アドレス不定の接続相手「peer1」、「peer2」との接続を想定しています。peer1 とのネゴシエーションでは事前共有鍵「1」を、peer2 とは「2」を使って認証を行います。この場合、相手側では自分の ID を「LOCALID="peer1"」のように指定します。

```
CREATE ISAKMP POLICY=c1 PEER=ANY KEY=1 REMOTEID=peer1 MODE=AGGRESSIVE
SENDN=TRUE ↵
CREATE ISAKMP POLICY=c2 PEER=ANY KEY=2 REMOTEID=peer2 MODE=AGGRESSIVE
SENDN=TRUE ↵
```

片側アドレスが不定なときに相手を認証する方法としてはもう 1 つ、XAUTH(Extended Authentication、拡張認証)と呼ばれる方法があります。これは、フェーズ 1 完了後、フェーズ 2 の開始前にユーザー名/パスワードなどの認証を行う方式です。

アドレス固定側では、PEER パラメーターに ANY、XAUTH パラメーターに SERVER (認証を要求する側) を指定した ISAKMP ポリシーを 1 つだけ作成します。また、相手のユーザー名とパスワードをユーザー認証データベース等に登録しておきます。

```
CREATE ISAKMP POLICY=i PEER=ANY KEY=1 SENDN=TRUE XAUTH=SERVER ↵
ADD USER=client1 PASSWORD=passclie1 LOGIN=NO ↵
ADD USER=client2 PASSWORD=passclie2 LOGIN=NO ↵
... ↵
```

アドレス不定側では、XAUTH パラメーターに CLIENT (認証を受ける側) を指定します。また、自分のユーザー名とパスワードも指定します。フェーズ 1 の事前共有鍵は XAUTH 認証を受けるすべてのクライアントで共通になります。個々のクライアントの認証はフェーズ 1 完了後の XAUTH によって行われます。

```
CREATE ISAKMP POLICY=i PEER=1.1.1.1 KEY=1 SENDN=TRUE XAUTH=CLIENT ↵
SET ISAKMP POLICY=i XAUTHNAME=client1 XAUTHPASS=passclie1 ↵
```

相手認証に RSA デジタル署名方式を使用する場合は、AUTHTYPE パラメーターに RSASIG を指定し、LOCALRSAKEY パラメーターで自分の公開鍵ペアの番号を指定します。

```
CREATE ISAKMP POLICY=i PEER=2.2.2.2 AUTHTYPE=RSASIG LOCALRSAKEY=2
SENDN=TRUE ↵
```

RSA デジタル署名を利用した IPsec の設定方法については「PKI」の章をご覧ください。

フェーズ 1 の鍵交換で使用する Diffie-Hellman (Oakley) グループを変更するには、GROUP パラメーターを使います。省略時はグループ 1 (768 ビット MODP) です。

```
CREATE ISAKMP POLICY=i PEER=2.2.2.2 KEY=1 SENDN=TRUE GROUP=2 ↵
```

ISAKMP ポリシーの設定内容は、SHOW ISAKMP POLICY コマンド (122 ページ) で確認できます。

```
SHOW ISAKMP POLICY ↵
SHOW ISAKMP POLICY=i ↵
```

手動鍵管理

ISAKMP/IKE を使わない場合は、SA (SA スペック) ごとに手動で鍵 (暗号鍵と認証鍵) と SPI (外向き、内向き) を設定する必要があります。

鍵の作成は CREATE ENCO KEY コマンド (「暗号・圧縮」の 18 ページ) で行います。SA で使用する鍵はすべて共有鍵ですので、対向機器間で同じ値を使用するようにしてください。鍵の作成方法については「暗号・圧縮」の章をご覧ください。

鍵と SPI の指定は、CREATE IPSEC SASPECIFICATION コマンド (43 ページ) で行います。詳細は「SA スペック」をご覧ください。

その他

UDP トンネリング (ESP over UDP)

UDP トンネリング (ESP over UDP) は、IPsec パケット (ESP) を UDP パケットにカプセル化して送受信する本製品独自の機能です。この機能を使うと、ルーター間に NAT 機器が存在する場合でも IPsec を利用できます。

- ただし、NAT によって IP ヘッダーが変更されるため、セキュリティープロトコルとして AH を使うことはできません。これは、AH のデータ認証範囲が外側 IP ヘッダー (の一部) を含むためです。

UDP トンネリングを使用するには、「ACTION=IPSEC」の IPsec ポリシーで「UDPTUNNEL=TRUE」を指定します。これにより、UDP の 2746 番ポートで ESP over UDP パケットの送受信を行うようになります。両側のルーターとも UDP トンネリングを有効にしてください。

```
SET IPSEC POLICY=vpn UDPTUNNEL=TRUE ↵
```

NAT 機器の背後に位置するルーターでは、さらに次のコマンドを実行して UDP ハートビートを有効にします。UDP ハートビートは、NAT 機器の変換テーブルからセッション情報が削除されないよう、30 秒ごとに相手ルーター宛てに送信されるパケットです。セッション保持だけを目的とするため、受信しても特別な処理は行われません。

```
SET IPSEC POLICY=vpn UDPHEARTBEAT=TRUE ↵
```

UDP トンネリングを使用するときは、両側のルーターに以下の IPsec ポリシーを追加し、ESP over UDP パケットを通過させるようにしてください。本ポリシーは、IPsec を適用するポリシー（ACTION=IPSEC）よりも前に置いてください（ISAKMP パケットを通過させるポリシーと同様）。

```
CREATE IPSEC POLICY=udp INT=ppp0 ACTION=PERMIT LPORT=2746 TRANSPORT=UDP ↵
```

UDP トンネリングパケット（ESP over UDP）は、送受信とも UDP ポート 2746 番を使います。ポート番号を変更するには、SET IPSEC UDPPORT コマンド（83 ページ）および、CREATE IPSEC POLICY コマンド（39 ページ）/SET IPSEC POLICY コマンド（78 ページ）の UDPPORT パラメーターを使います。ローカル側ポートを変更するには、SET IPSEC UDPPORT コマンド（83 ページ）を使います。これにより、3456 番ポートで UDP トンネリングパケットを受信するようになります。また、送信時も 3456 番ポートから送出します。

```
SET IPSEC UDPPORT=3456 ↵
```

リモート側ポートは相手ルーターごとに設定する必要があるため、IPsec ポリシーのパラメーターとして設定します。これにより、IPsec ポリシー「vpn」では、UDP トンネリングパケットを相手ルーター（PEER）の 3456 番ポートに送信します。

```
SET IPSEC POLICY=vpn UDPPORT=3456 ↵
```

- ＼ UDP ポートを変更したときは、トンネリングパケットを通過させる IPsec ポリシーの条件も忘れずに変更してください。

ファイアウォールを使用しているときは、WAN 側からのトンネリングパケットを通過させるルールを追加してください。詳細は「IPsec とファイアウォールの併用」をご覧ください。

IPsec とファイアウォールの併用

IPsec ルーター上でファイアウォールを有効にしているときは、ISAKMP パケットや IPsec パケットがファイアウォールで遮断されないよう、ルールを追加する必要があります。

また、ファイアウォール NAT を使っている場合は、プライベート LAN 間のパケットに NAT が適用されないようにすることも必要です。

以下、前述の「基本構成」をもとに、IPsec とファイアウォールを併用するための設定方法を説明します。ここでは、さきほどの「基本構成」に、次のようなファイアウォールの設定を追加したものと仮定します。これは、LAN 側からのパケットはすべて通過させ、WAN 側からのパケットはすべて拒否するファイアウォールの基本設定です。また、LAN 側コンピューターがインターネットにアクセスできるよう、WAN 側インターフェースのグローバルアドレスを利用したダイナミック ENAT の設定も含まれています。

```
ENABLE FIREWALL
CREATE FIREWALL POLICY=net
ENABLE FIREWALL POLICY=net ICMP_F=ALL
DISABLE FIREWALL POLICY=net IDENTPROXY
ADD FIREWALL POLICY=net INT=eth0 TYPE=PRIVATE
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0
```

このようなファイアウォール設定をすると、IPsec 通信に必要なパケットまで遮断されてしまうため、IPsec の通信ができなくなります。IPsec を使う場合は、ご使用の環境に応じて以下の設定を追加してください。

ISAKMP/IKE を使っている場合は、相手ルーターからの ISAKMP パケットが遮断されないように次のようなルールを設定します（ルーターの UDP500 番宛てパケットを許可）。

```
ADD FIREWALL POLICY=net RULE=1 ACTION=ALLOW INT=ppp0 PROT=UDP GBLPORT=500
    GBLIP=1.1.1.1 PORT=500 IP=1.1.1.1 ↵
```

UDP トンネリングを使っている場合は、ISAKMP パケットと同様、ESP パケットをカプセル化している UDP パケット（ESP over UDP）も通すように設定します（ルーターの UDP2746 番宛てパケットを許可）。

```
ADD FIREWALL POLICY=net RULE=2 ACTION=ALLOW INT=ppp0 PROT=UDP
    GBLPORT=2746 GBLIP=1.1.1.1 PORT=2746 IP=1.1.1.1 ↵
```

ローカル LAN からリモート LAN へのパケットに NAT が適用されないよう、次のようなルールを追加します。このルールは、「eth0 で受信した IP パケットのうち、始点が 192.168.10.1～192.168.10.254 の範囲で、終点が 192.168.20.1～192.168.20.254 の範囲ならば NAT をかけない」の意味になります。

```
ADD FIREWALL POLICY=net RULE=3 ACTION=NONAT INT=eth0 PROT=ALL
    IP=192.168.10.1-192.168.10.254 ↵
SET FIREWALL POLICY=net RULE=3 REMOTEIP=192.168.20.1-192.168.20.254 ↵
```

相手ルーターから送られてきた IPsec パケットが遮断されないよう、次のようなルールを追加します。「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。したがって、以下のコマンドは、「ppp0 で受信した IPsec パケットから取り出したパケットの終点が 192.168.10.1～192.168.10.254 の範囲、すなわちローカル側 LAN 宛てならば NAT 変換の対象外とする」の意味になります。

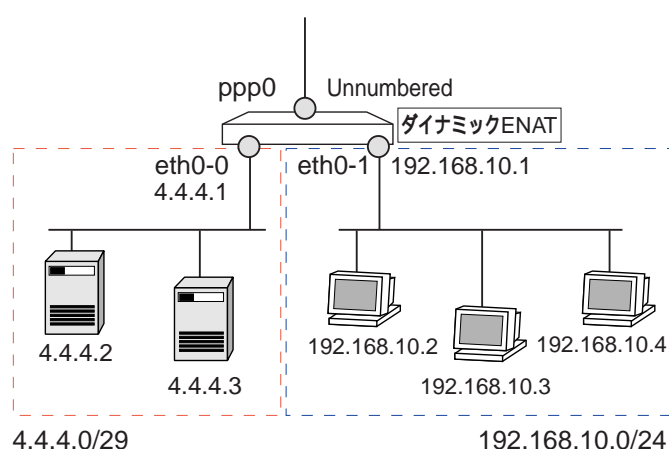
```
ADD FIREWALL POLICY=net RULE=4 ACTION=NONAT INT=ppp0 PROT=ALL
    IP=192.168.10.1-192.168.10.254 ENCAP=IPSEC ↵
```

Unnumbered IP インターフェース使用時の注意

IPsec を使うときは、IP パケットの始点アドレスとしてルーター自身のアドレスが使われるため、IPsec ポリシーを適用する WAN 側インターフェースが Unnumbered の場合は、いくつか注意すべきことがあります。IPsec パケットを送出するインターフェースが Unnumbered の場合、始点アドレスとして有効なアドレスがないため、その他のインターフェースの中で一番最初に設定されたアドレスが始点アドレスとして使用されます。

WAN 側 Unnumbered のときは、通常 LAN 側に ISP から割り当てられたグローバルを設定しますが、このとき IPsec パケットの始点として使いたいアドレスを最初に ADD IP INTERFACE コマンド（「IP」の 175 ページ）で設定するよう注意してください。

このような問題が発生するのは次のような構成のときです。



この構成では、WAN 側インターフェース（ppp0）が Unnumbered になっています。そのため、ppp0 から送られる IPsec パケットや ISAKMP パケットの始点アドレスには、他のインターフェースの中で最初に設定されたアドレスが使用されます。

そのため次の順序でアドレスを設定すると、ルーター自身が送信するパケットでは始点アドレスとして 192.168.10.1 が使われてしまい、インターネット上での通信ができなくなってしまいます。

```
ADD IP INT=eth0-1 IP=192.168.10.1 MASK=255.255.255.0 ↵
```

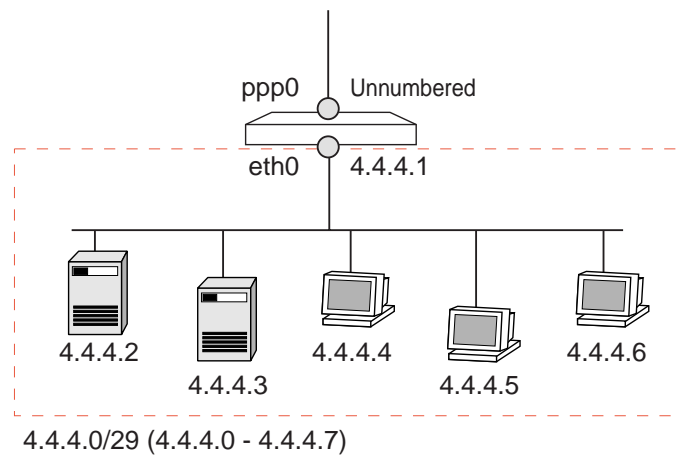
```
ADD IP INT=eth0-0 IP=4.4.4.1 MASK=255.255.255.248 ↵
```

このような状況を避けるため、このケースでは次の順序でアドレスを設定するよう注意してください。これにより、4.4.4.1 が始点アドレスとして使われるようになります。

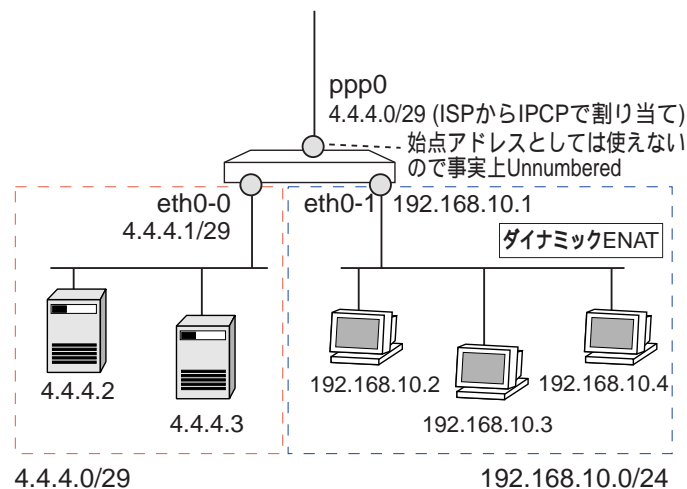
```
ADD IP INT=eth0-0 IP=4.4.4.1 MASK=255.255.255.248 ↵
```

```
ADD IP INT=eth0-1 IP=192.168.10.1 MASK=255.255.255.0 ↵
```

なお、次のような構成では、WAN 側が Unnumbered であってもその他のアドレスが 1 つしかないため、上記のような問題は発生しません。



PPPoE LAN 型接続では、WAN 側 Unnumbered というものの、実際には Unnumbered ではなく、ネットワークアドレスが WAN 側に割り当てられるケースがあるようです。この場合は、始点アドレスとして WAN 側インターフェースに設定されたネットワークアドレス（ホストアドレスとしては無効）を使うため、他のインターフェースのアドレスが始点になるよう設定を工夫してください。次のような構成を例に解説します。



IPsec 等を使わない場合（ルーター自身がインターネット側にパケットを送信することがない場合）は、次のように設定しても問題ありません。ppp0 のアドレスはホストアドレスとしては無効なため、実質的には Unnumbered になります。

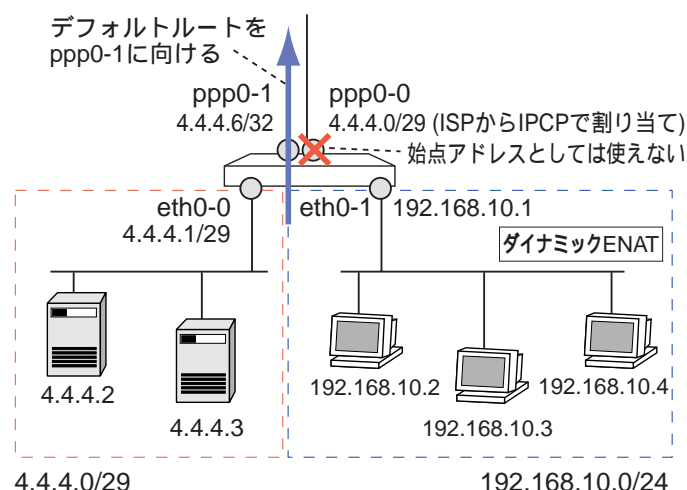
```

ENABLE IP ↓
ENABLE IP REMOTEASSIGN ↓
ADD IP INT=ppp0 IP=0.0.0.0 ↓
ADD IP INT=eth0-0 IP=4.4.4.1 MASK=255.255.255.248 ↓
ADD IP INT=eth0-1 IP=192.168.10.1 MASK=255.255.255.0 ↓
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXT=0.0.0.0 ↓

```

しかし、IPsec を使う場合は前記のような問題が発生します。この設定では、IPsec パケットが ppp0 から送出されますが、このケースでは ppp0 が純粋な Unnumbered でないため、ホストアドレスとしては本来無効なはずのネットワークアドレス (4.4.4.0) が始点アドレスとして使われてしまいます。そのため、ISP 側のルーターでパケットが破棄され IPsec の通信ができなくなります。

これを回避するためには、WAN 側インターフェースをマルチホーミングして有効なホストアドレスを設定し、デフォルトルートが有効なアドレスを持つインターフェースを向くように設定します。



```

ENABLE IP ↓
ENABLE IP REMOTEASSIGN ↓
ADD IP INT=ppp0-0 IP=0.0.0.0 ↓
ADD IP INT=ppp0-1 IP=4.4.4.6 MASK=255.255.255.255 ↓
ADD IP INT=eth0-0 IP=4.4.4.1 MASK=255.255.255.248 ↓
ADD IP INT=eth0-1 IP=192.168.10.1 MASK=255.255.255.0 ↓
ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXT=0.0.0.0 ↓

```

この場合、アドレスが 1 つ無駄になりますが、IPsec パケットが ppp0-1 から送出されるため、始点アドレスとして有効な 4.4.4.6 が使われるようになります。

動作・設定の確認

IPsec の動作や設定を確認する場合、あるいは、IPsec の通信ができない場合は、以下の各項目をチェックしてみてください。

基本的な情報

最初に IPsec モジュールが有効になっているかどうかを確認します。SHOW IPSEC コマンド (88 ページ) を実行し、Module Status が ENABLED になっているかどうか確認してください。

```
SHOW IPSEC ↓
```

ISAKMP を使っているときは、ISAKMP モジュールが有効になっているかどうか確認してみましょう。SHOW ISAKMP コマンド (114 ページ) を実行し、Module Status が ENABLED になっているかどうか確認してください。

```
SHOW ISAKMP ↓
```

自動鍵管理 (ISAKMP/IKE) を使っているときは、IPsec SA のネゴシエーション (フェーズ 2) に先立ち、ISAKMP SA のネゴシエーションが行われます (フェーズ 1)。SHOW ISAKMP SA コマンド (126 ページ) で ISAKMP SA が確立されているかどうかを確認してください。

```
SHOW ISAKMP SA ↓
```

```
SecOff > show isakmp sa
```

				Expiry Limits - hard/soft/used	
SA Id	PeerAddress	EncA.	HashA.	Bytes	Seconds

3	1.1.1.1	DES	SHA	-/-/-	86400/82080/1382

ISAKMP SA の確立に失敗するおもな原因は、事前共有鍵 (pre-shared key) や ISAKMP ポリシーの設定ミスです。事前共有鍵が両方のルーターで同じに設定されているか、各ルーターの ISAKMP ポリシーに矛盾がないかを確認してください。

```
SHOW ENCO KEY=1 ↓
```

```
SHOW ISAKMP POLICY ↓
```

```
SHOW ISAKMP POLICY=i ↓
```

```
SHOW CONFIG DYNAMIC=ISAKMP ↓
```

ISAKMP 関連のイベントはログにも記録されます。必要に応じてログを確認してください。ISAKMP SA や IPsec SA の確立に成功していれば、「Exchange n: Completed successfully」のようなメッセージが記録されているはずです。

```
SHOW LOG MODULE=ISAK ↓
```

または

SHOW LOG TYPE=IKMP ↓

```
SecOff > show log module=isak

Date/Time    S Mod  Type  SType Message
-----
03 11:22:49 3 ISAK IKMP  MSG   ISAKMP has been enabled
03 11:31:10 3 ISAK IKMP  XCHG  Exchange 1: Phase 1 [init] started with peer
                2.2.2.2
03 11:31:14 3 ISAK IKMP  XCHG  Exchange 1: Notification Received - DOI
03 11:31:14 3 ISAK IKMP  XCHG  Exchange 1: Completed successfully
03 11:31:14 3 ISAK IKMP  XCHG  Exchange 2: Phase 2 [init] started with peer
                2.2.2.2
03 11:31:14 3 ISAK IKMP  XCHG  Exchange 2: Completed successfully
-----
```

SHOW ISAKMP EXCHANGE コマンド (118 ページ) を実行すると、完了していない ISAKMP ネゴシエーションがあるかどうかを確認できます。いつになっても、同じ情報が表示されるときは、ネゴシエーションが途中で止まってしまっている可能性が大了。通常は、このコマンドを実行しても何も表示されません。

SHOW ISAKMP EXCHANGE ↓

```
SecOff > show isakmp exchange

ISAKMP Exchanges

  Id  Phase  State      PeerAddress      Type
-----
   3    4  WAIT_HASH_SA_NONCE 2.2.2.2          QUICK
```

IPsec 通信が行われるためには、ルーター間に IPsec SA が確立されている必要があります。IPsec SA は使用するプロトコルごとに用意します。IPsec SA は、自動鍵管理では ISAKMP/IKE のネゴシエーション (フェーズ 2) によって自動的に確立されます。一方、手動鍵のときは、管理者が固定的に設定します。SHOW IPSEC SA コマンド (104 ページ) で IPsec SA が確立されているかどうかを確認してください。

SHOW IPSEC SA ↓

```
SecOff > show ipsec sa

SA Id  Policy      Bundle  State  Protocol  OutSPI  InSPI
-----
   2  v1          1  Valid  ESP       3154027431 4241764757
   3  v1          1  Valid  AH        1252362122 3221961085
   4  vf3         1  Valid  ESP       28060662  981246197
   5  vf1         1  Valid  ESP       51507534  3371320620
```

また、IPsec SA バンドルの情報は SHOW IPSEC POLICY コマンド (96 ページ) の SABUNDLE オプションで確認できます。

```
SecOff > show ipsec policy sabundle
```

Ipsec Policy SA Bundles

Bundle	SA's	State	Expiry Limits - hard/soft/used Bytes	Seconds
Policyv1				
0	2,3	VALID	-/-/1728	28800/27360/2732
Policyvx1				
Policyvf1				
0	5	VALID	-/-/220	28800/27360/2004
Policyvf2				
Policyvf3				
0	4	VALID	-/-/440	28800/27360/2052

ISAKMP/IKE で IPsec SA の確立に失敗するおもな原因は、IPsec の設定 (SA スペック、バンドルスペック、IPsec ポリシー) が両方のルーターで食い違っていることです。次の各コマンドで両方のルーターの設定に矛盾がないか確認してください。また、前述の手順にしたがい、SHOW ISAKMP SA コマンド (126 ページ) で ISAKMP SA が確立されているかどうか確認してください。ISAKMP SA が確立されていないと IPsec SA のネゴシエーション自体が行えません。

```
SHOW IPSEC SASPECIFICATION ↓
```

```
SHOW IPSEC BUNDLESPECIFICATION ↓
```

```
SHOW IPSEC POLICY ↓
```

```
SHOW CONFIG DYNAMIC=IPSEC ↓
```

また、手動鍵の場合も上記のコマンドを実行して、ルーター間で SA やポリシーに矛盾がないか確認してください。

IPsec 関連のイベントはログにも記録されます。必要に応じてログを確認してください。

```
SHOW LOG MODULE=IPSE ↓
```

または

```
SHOW LOG TYPE=IPSC ↓
```

```
SecOff > show log type=ipsc
```

Date/Time	S	Mod	Type	SType	Message

```

17 07:54:36 3 IPSE IPSC MSG   IPSEC has been enabled
17 07:55:29 3 IPSE IPSC MSG   SA bundle created: Policy - vl
17 08:11:28 3 IPSE IPSC MSG   SA bundle created: Policy - vf3
17 08:12:17 3 IPSE IPSC MSG   SA bundle created: Policy - vf1
-----

```

デバッグオプション

ISAKMP のデバッグオプションを有効にすると、ISAKMP パケットの処理が行われるたびに、コンソールにデバッグ情報が表示されます。デバッグオプションを有効にするには、ENABLE ISAKMP DEBUG コマンド (64 ページ) を使います。

```
ENABLE ISAKMP DEBUG={ALL|DEFAULT|PACKET|PKT|PKTRAW|STATE|TRACE|TRACEMORE} ↵
```

次に PKT オプションを有効にしたときの画面表示例を示します。PKT は、ルーターが送受信する ISAKMP メッセージをデコードして詳細に表示するオプションです。ISAKMP/IKE ネゴシエーションの様子を詳しく観察することができます。

```

SecOff > enable isakmp debug=pkt

Info (182057): ISAKMP Debugging has been enabled.

SecOff > ISAKMP Tx Message
  Cookie's:      5052045c2e566b81:0000000000000000
  Xchg Type:     IDPROT(2)  Ver: 10  Flags: 00
  MessageID:     00000000   Total Length: 84
  Payload #:     0   Length: 56   Type: Security Association (SA)
    DOI: IPSEC(0)  Situation: 00000001
      Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
        Transform#: 1
          Transform Id ..... IKE(1)
          Encryption Algorithm..... DES(1)
          Authentication Algorithm..... SHA(2)
          Authentication Method..... PRESERVED(1)
          Group Description..... 768(1)
          Group Type..... MODP
          Expiry Seconds..... 86400

```

IPsec ポリシーのデバッグオプションを有効にすると、IP パケットに対して IPsec の処理が行われるたびに、コンソールにデバッグ情報が表示されます。デバッグオプションを有効にするには、ENABLE IPSEC POLICY DEBUG コマンド (59 ページ) を使います。

```
ENABLE IPSEC POLICY=policy DEBUG={FILTER|PACKET|TRACE|ALL} ↵
```

```

SecOff > ena ipsec policy=vpn debug=packet

Info (181057): IPSEC Policy Debugging has been enabled.

```



```
SecOff >
IPSEC vpn: 2: OUT: pre processing:
IP: 45000028eb1040002006d908c0a81464c0a80102
TCP: 0429005005b7e65c01faee4c5004000038560000
data:

IPSEC vpn: 2: OUT: post processing:
IP: 450000604b7f00004032fa573f0c42ef01010101
ESP: 14f45fa300000b09:35d26e02458706623d9aa9bf
data: 9fcd18d0a34ffeeeb8b0f574ddea820f8ba0db36cd7a9fc0254f08215e2aa7ecdb34688
6193f17d39cc7f096276238bf262b668920b51c535d26e02458706623d9aa9bf
```

統計カウンター

以下の各コマンドでは、IPsec や ISAKMP に関する統計カウンターを確認することができます。多くのカウンターはルーターの内部処理にかかわる非常に細かい情報ですが、通信上のトラブルシューティングに役立つものもあります。

IPsec の全般的な動作に関するカウンターは SHOW IPSEC COUNTERS コマンド (91 ページ) で確認できます。COUNTERS パラメーターで特定のカウンターだけを表示させることもできます。

```
SHOW IPSEC COUNTERS ↓
```

ISAKMP 関連の統計カウンターは SHOW ISAKMP COUNTERS コマンド (116 ページ) で確認できます。

```
SHOW ISAKMP COUNTERS ↓
```

ISAKMP SA のネゴシエーション (フェーズ 1) に失敗する場合は、Main モード (MODE=MAIN のとき。デフォルト) または Aggressive モード (MODE=AGGRESSIVE) のカウンターに注目してください。

```
SHOW ISAKMP COUNTERS=MAIN ↓
```

```
SHOW ISAKMP COUNTERS=AGGRESSIVE ↓
```

ISAKMP SA は確立できたが、IPsec SA のネゴシエーション (フェーズ 2) に失敗する場合は、QUICK モードのカウンターに注目してください。

```
SHOW ISAKMP COUNTERS=QUICK ↓
```

それぞれの IPsec ポリシーでどのような処理が何回行われたかは、SHOW IPSEC POLICY コマンド (96 ページ) の COUNTERS オプションで確認できます。

```
SHOW IPSEC POLICY=vpn COUNTERS ↓
```

IPsec SA の統計カウンターは、SHOW IPSEC SA コマンド (104 ページ) の COUNTERS オプションで確認できます。

```
SHOW IPSEC SA ↵
```

```
SHOW IPSEC SA=2 ↵
```

コマンドリファレンス編

機能別コマンド索引

一般コマンド

DISABLE IPSEC	53
ENABLE IPSEC	58
PURGE IPSEC	72
RESET IPSEC COUNTER	73
RESET IPSEC SA COUNTER	75
SET IPSEC UDPPORT	83
SHOW IPSEC	88
SHOW IPSEC COUNTERS	91
SHOW IPSEC SA	104

IPsec ポリシー

CREATE IPSEC POLICY	39
DESTROY IPSEC POLICY	50
DISABLE IPSEC POLICY DEBUG	54
ENABLE IPSEC POLICY DEBUG	59
RESET IPSEC POLICY COUNTER	74
SET IPSEC POLICY	78
SHOW IPSEC POLICY	96

SA スペック

CREATE IPSEC SASPECIFICATION	43
DESTROY IPSEC SASPECIFICATION	51
SET IPSEC SASPECIFICATION	81
SHOW IPSEC SASPECIFICATION	111

SA バンドルスペック

CREATE IPSEC BUNDLESPECIFICATION	37
DESTROY IPSEC BUNDLESPECIFICATION	49
SET IPSEC BUNDLESPECIFICATION	77
SHOW IPSEC BUNDLESPECIFICATION	89

ISAKMP

CREATE ISAKMP POLICY	45
DESTROY ISAKMP POLICY	52
DISABLE ISAKMP	56
DISABLE ISAKMP DEBUG	57
ENABLE ISAKMP	62
ENABLE ISAKMP DEBUG	64

RESET ISAKMP COUNTER	76
SET ISAKMP POLICY	84
SHOW ISAKMP	114
SHOW ISAKMP COUNTERS	116
SHOW ISAKMP EXCHANGE	118
SHOW ISAKMP POLICY	122
SHOW ISAKMP SA	126

CREATE IPSEC BUNDLESPECIFICATION

カテゴリー：IPsec / SA バンドルスペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
CREATE IPSEC BUNDLESPECIFICATION=bspec-id KEYMANAGEMENT={ISAKMP|MANUAL}
    STRING="bundle-string" [EXPIRYKBYTES=1..2000000000]
    [EXPIRYSECONDS=300..31449600]
```

bspec-id: SA バンドルスペック番号 (0~255)

bundle-string: SA スペック指定文字列 (1~100 文字。SA スペック番号 (0~255) をセパレーター (AND、OR、カンマ) で区切って並べたもの)

解説

SA バンドルスペックを作成する。

SA バンドルスペックは、IPsec 通信で使用する SA スペック (プロトコル等) の組み合わせを指定するもの。これにより、あるトラフィックには暗号化 (ESP) と認証 (AH) を施し、別のトラフィックには圧縮 (IPComp) と暗号化 (ESP) を適用するといった設定が可能になる。

パラメーター

BUNDLESPECIFICATION SA バンドルスペック番号

KEYMANAGEMENT 鍵管理方式。SA バンドルの作成を手動で行うか (MANUAL=手動鍵管理)、ISAKMP/IKE のネゴシエーションによって自動的に行うか (ISAKMP=自動鍵管理) を指定する。

STRING バンドルを構成する SA スペックの組み合わせ。SA スペック番号を AND、OR、カンマで区切って記述する。手動鍵管理の場合は、最大 3 個の SA スペックを AND で区切って指定する。各 SA スペックは、それぞれ別の IPsec プロトコル (ESP、AH、IPComp) でなくてはならない。たとえば、SA スペック「1」(IPComp) と「3」(ESP) からなる SA バンドルは「1 AND 3」のように指定する。この場合、パケットに対して IPComp、ESP の順に処理が行われる。自動鍵管理の場合は、SA スペックの組み合わせをカンマ区切りで複数候補指定できる。実際にどのバンドル構成が使用されるかは、ISAKMP/IKE のネゴシエーションによって決まる。SA スペック「1」と「2」なら「1 AND 2」、「1」か「2」のどちらかのみなら「1 OR 2」、「1」と「2」が第一候補で「1」と「3」が第二候補なら、「1 AND 2, 1 AND 3」のように記述する。「AND」は併用するプロトコルを指定するものでそれぞれが異なるプロトコルでなくてはならない。「OR」はアルゴリズムの選択肢を示すもので同じプロトコルでなくてはならない。また、「AND」によるプロトコルの適用順序は、通常 IPComp、ESP、AH の順とする。IPComp は必ず先頭でなくてはならない。

EXPIRYKBYTES バンドル内 SA の有効期限 (Kbyte)。通信データ量がここで指定した量に達すると、該当 SA バンドルは再ネゴシエートされる。KEYMANAGEMENT パラメーターに ISAKMP を指定したときだけ有効。デフォルトは無期限。

EXPIRYSECONDS バンドル内 SA の有効期限 (秒)。バンドル作成後ここで指定した時間が経過すると、該当 SA バンドルは再ネゴシエートされる。KEYMANAGEMENT パラメーターに ISAKMP を指定

したときだけ有効。デフォルトは 28800 秒（8 時間）。

例

手動鍵管理用の SA バンドルスペック「1」を作成する。SA スペックは「1」と「2」を使用する。

```
CREATE IPSEC BUNDLE=1 KEYMAN=MANUAL STRING="1 AND 2"
```

自動鍵管理用の SA バンドルスペック「2」を作成する。SA スペックの組み合わせは、3 つの候補を指定する。

```
CREATE IPSEC BUNDLE=2 KEYMAN=ISAKMP STR="1 OR 2 AND 4, 1 OR 2, 3 AND 4"
```

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DESTROY IPSEC BUNDLESPECIFICATION（49 ページ）

SET IPSEC BUNDLESPECIFICATION（77 ページ）

SHOW IPSEC BUNDLESPECIFICATION（89 ページ）

CREATE IPSEC POLICY

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
CREATE IPSEC POLICY=policy INTERFACE=interface ACTION={DENY|IPSEC|
PERMIT} [KEYMANAGEMENT={ISAKMP|MANUAL}] [BUNDLESPECIFICATION=bspec-id]
[PEERADDRESS={ipadd|ANY|DYNAMIC}] [LADDRESS={ANY|ipadd[-ipadd]}]
[LMASK=ipadd] [LNAME={ANY|system-name}] [LPORT={ANY|port}]
[RADDRESS={ANY|ipadd[-ipadd]}] [RMASK=ipadd] [RNAME={ANY|system-name}]
[RPORT={ANY|port}] [TRANSPORTPROTOCOL={ANY|ESP|GRE|ICMP|OSPF|RSVP|TCP|
UDP|protocol}] [DFBIT={SET|COPY|CLEAR}] [GROUP={0|1|2}]
[IPROUTETEMPLATE=template] [ISAKMPPOLICY=isakmp-policy]
[SRCINTERFACE=interface] [UDPHEARTBEAT={TRUE|FALSE}] [UDPPORT=port]
[UDPTUNNEL={TRUE|FALSE}] [USEPFSKEY={TRUE|FALSE}] [POSITION=pos]
```

policy: IPsec ポリシー名 (1~23 文字)

interface: IP インターフェース名 (eth0、ppp0 など)

bspec-id: SA バンドルスペック番号 (0~255)

ipadd: IP アドレスまたはネットマスク

system-name: システム名 (1~120 文字。空白を含む場合はダブルクォートで囲む)

port: TCP/UDP ポート番号 (0~65535)

protocol: IP プロトコル番号 (0~255)

template: ルートテンプレート名 (1~31 文字。大文字小文字を区別しない)

isakmp-policy: ISAKMP ポリシー名 (1~24 文字。空白を含む場合はダブルクォートで囲む)

pos: ポリシールールの位置 (1~50)

解説

IPsec ポリシーを作成する。

IPsec ポリシーは、IP アドレス・IP プロトコル・ポートなどによって識別されるパケットに対し、どのような処理 (IPsec 適用、通過、拒否) を施すかを指定する一種のフィルタールール。

IPsec ポリシーは IP インターフェースごとに管理され、作成順または POSITION パラメーターで指定した順番で検索される。インターフェースに対して 1 つでもポリシーを作成すると、ポリシーリストの末尾にすべてのパケットを破棄 (DENY) する暗黙のポリシーが作成されるので注意が必要。

IPsec ポリシーが設定されているインターフェースでパケットを送受信する際、該当インターフェースに設定されている IPsec ポリシーが POSITION 番号の若い順に検索され、最初にマッチしたポリシーで指定されている処理 (ACTION) が実行される。

パラメーター

POLICY IPsec ポリシー名

INTERFACE このポリシーを適用するインターフェース名。IPsec ポリシーは、指定したインターフェースからパケットを送出するときと、同インターフェースでパケットを受信したときに処理される。通

常は WAN 側のインターフェースを指定する

ACTION 本ポリシーの条件(LADDRESS、LMASK、LNAME、LPORT、RADDRESS、RMASK、RNAME、RPORT、TRANSPORTPROTOCOL)に適合したパケットに対する処理を指定する。IPSEC(BUNDLESPECIFICATION パラメーターで指定した SA バンドルによって処理する)、PERMIT (IPsec を使わない通常のパケット処理を行う)、DENY (パケットを破棄する) から選択する。IPSEC を指定した場合は、対向 IPsec 装置の IP アドレス (PEERADDRESS)、SA バンドルスペック (BUNDLESPECIFICATION)、鍵管理方式 (KEYMANAGEMENT) も指定すること

KEYMANAGEMENT SA バンドル作成時の鍵管理方式を指定する。手動(MANUAL)、自動(ISAKMP) から選択する。BUNDLESPECIFICATION パラメーターで指定した SA バンドルスペックと同じ方式を指定すること。ACTION に IPSEC を指定した場合のみ有効 (かつ必須)

BUNDLESPECIFICATION SA バンドル作成時に用いる SA バンドルスペックを指定する。SA バンドルは、IPsec で使用するセキュリティプロトコルやアルゴリズムの情報をひとまとめにしたもの。本パラメーターは、ACTION に IPSEC を指定した場合のみ有効 (かつ必須)。なお、SA バンドルスペックの鍵管理方式が、本コマンドの KEYMANAGEMENT パラメーターと一致していること

PEERADDRESS 対向 IPsec 装置の IP アドレス。相手の IP アドレスが不定かつ動的に変化する場合は DYNAMIC を指定する。また、任意の固定 IP アドレスの相手と接続する場合は ANY を指定する。DYNAMIC と ANY は、KEYMANAGEMENT に ISAKMP を指定した場合のみ有効

LADDRESS パケット選択パラメーター (セレクター) の 1 つ。ポリシーの適用対象となるパケットのローカル側 IP アドレスを指定する。LMASK と組み合わせてサブネットを指定したり、ハイフンでアドレスの範囲を指定することもできる。省略時は ANY (すべて)

LMASK セレクターの 1 つ。LADDRESS に対するネットマスクを指定する。省略時は 255.255.255.255

LNAME セレクターの 1 つ。ローカル側システム名を指定する。本パラメーターは自アドレスが不定のときに指定するもので、ISAKMP のフェーズ 2 ID として対向装置に送信される。省略時は ANY (すべて)

LPORT セレクターの 1 つ。ローカル側ポート番号。省略時は ANY (すべて)

RADDRESS セレクターの 1 つ。ポリシーの適用対象となるパケットのリモート側 IP アドレス。RMASK と組み合わせてサブネットを指定したり、ハイフンでアドレスの範囲を指定することもできる。省略時は ANY (すべて)

RMASK セレクターの 1 つ。RADDRESS に対するネットマスク。省略時は 255.255.255.255

RNAME セレクターの 1 つ。リモート側システム名を指定する。本パラメーターは対向装置のアドレスが不定のときに指定するもので、相手の ISAKMP のフェーズ 2 ID を指定する。省略時は ANY (すべて)

RPORT セレクターの 1 つ。リモート側ポート番号。省略時は ANY (すべて)

TRANSPORTPROTOCOL セレクターの 1 つ。ポリシーの適用対象となるパケットの IP プロトコルタイプ。ALL、TCP、UDP などの定義済み文字列か IP プロトコル番号で指定する。省略時は ANY (すべて)

DFBIT トンネルモード SA において、外側 IP ヘッダーの DF (Don't Fragment) ビットにどのような値を設定するかを指定する。COPY を指定した場合は、内側 IP ヘッダーの DF ビットの値をそのまま使用する。SET を指定した場合は、常にビットをオンにする。CLEAR を指定した場合は、常にビットをオフにする。インターネット上には異なる MTU を持つネットワークが混在しているため、DF ビットが立っているパケットはフラグメント不可により破棄される可能性があるため、通常は CLEAR を指定する。省略時は CLEAR

GROUP IKE フェーズ 2 (Quick モード) での Diffie-Hellman 鍵交換に使用する Oakley グループ。PFS (Perfect Forward Secrecy) を有効にしている場合 (USEPFSKEY パラメーターに TRUE を指定した場合) のみ有効。省略時はグループ 1

IPROUTETEMPLATE IP ルートテンプレート名。この IPsec ポリシーに基づいて IPsec SA が作成されたときに自動登録する経路エントリーのテンプレートを指定する。登録される経路の宛先アドレスは、IPsec SA のリモート側 IP アドレス/マスクとなる。本パラメーターは、ACTION が IPSEC で、PEERADDRESS が ANY か DYNAMIC のときのみ有効。省略時はなし

ISAKMPPOLICY ISAKMP ポリシー名。ACTION に IPSEC を指定した場合のみ有効。通常指定する必要はないが、同じ PEER を持つ ISAKMP ポリシーが複数存在するときに、この IPsec ポリシーで使用する ISAKMP ポリシーを明示的に指定したい場合に使う

SRCINTERFACE IPsec パケットの始点インターフェース。本パラメーターを指定した場合、IPsec パケットの始点アドレスにここで指定したインターフェースのアドレスが使用される。省略時は、パケットを送出するインターフェースのアドレスが使用される。送出インターフェースが Unnumbered の場合は、本パラメーターで始点アドレスを明示的に指定するとよい

UDPHEARTBEAT UDP ハートビートを使用するかどうか。UDP ハートビートは、UDP トンネリング (ESP over UDP) 使用時にセッション情報が NAT 機器の変換テーブルから消えてしまうことを防ぐ本製品の独自機能。TRUE を指定した場合は、対向 IPsec ルーターの UDP ポート 2746 番宛てに 30 秒間隔でハートビートパケットを送信する。このパケットはセッション維持だけを目的としているため、受信しても特別な処理は行われない。省略時は FALSE

UDPPORT UDP トンネリング (ESP over UDP) パケットの送信先 UDP ポート。デフォルトは 2746 番

UDPTUNNEL UDP トンネリング (ESP over UDP) を使用するかどうか。TRUE を指定した場合は、IPsec (ESP) パケットを UDP でカプセル化して対向ルーターの 2746 番ポート (UDPPORT パラメーターで変更可能) 宛てに送信する。これにより、IPsec 装置間に NAT 機器があるような環境でも IPsec を使用できる。ただし、AH は使用できない。省略時は FALSE

USEPFSKEY PFS (Perfect Forward Secrecy) の有効・無効。PFS とは、ある鍵の解読が他の鍵の解読の手がかりにならないような性質を言う。PFS を有効にすると、IPsec SA 鍵の生成・更新時に Diffie-Hellman アルゴリズムを再実行するようになる。自動鍵管理 (KEYMANAGEMENT=ISAKMP) のときのみ有効。省略時は FALSE

POSITION IPsec ポリシーリスト内における本ポリシーの位置。省略時はリストの最後尾に追加される。ポリシーリストは、適用インターフェース (INTERFACE) ごとに個別管理される

例

192.168.10.0/24・192.168.20.0/24 間のパケットに IPsec を適用するポリシー「vpn」を作成する。対向 IPsec ルーターのグローバル IP アドレスは 2.2.2.2、IPsec 処理の内容は SA バンドルスベック「1」で指定している。

```
CREATE IPSEC POLICY=vpn INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=2.2.2.2
SET IPSEC POLICY=vpn LAD=192.168.10.0 LMA=255.255.255.0 RAD=192.168.20.0
  RMA=255.255.255.0
```

アドレス不定の VPN クライアントから LAN 側ネットワーク (192.168.10.0/24) への VPN 接続を受け入れるポリシー「v1」を作成する。クライアントの識別は、相手が送ってくるフェーズ 2 ID (ここでは「user1」) によって行う。

```
CREATE IPSEC POLICY=v1 INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
  PEER=DYNAMIC
SET IPSEC POLICY=v1 LAD=192.168.10.0 LMA=255.255.255.0 RNAME=user1
```

他の IPsec ポリシーにマッチしなかったパケットをすべて素通し (平文通信) させる IPsec ポリシー「inet」を作成する。特定のサイトとは IPsec で通信し、その他のサイトとは平文で通信したい場合は、最後のポリシーとして「すべて許可」のポリシーを設定する必要がある (RAD などの条件を指定しなかった場合は「すべて」の意味になる)。

```
CREATE IPSEC POLICY=inet INT=ppp0 ACTION=PERMIT
```

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

```
ADD IP ROUTE TEMPLATE (「IP」の 187 ページ)
DESTROY IPSEC POLICY (50 ページ)
DISABLE IPSEC POLICY DEBUG (54 ページ)
ENABLE IPSEC POLICY DEBUG (59 ページ)
SET IPSEC POLICY (78 ページ)
SHOW IPSEC POLICY (96 ページ)
```

CREATE IPSEC SASPECIFICATION

カテゴリー：IPsec / SA スペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
CREATE IPSEC SASPECIFICATION=saspec-id KEYMANAGEMENT={ISAKMP|MANUAL}
    PROTOCOL={AH|COMP|ESP} [MODE={TRANSPORT|TUNNEL}] [COMPALGORITHM=LZS]
    [ENCALGORITHM={DES|3DESOUTER|NULL}] [ENCKEY=key-id] [HASHALGORITHM={MD5|
    NULL|SHA}] [HASHKEY=key-id] [INSPI=spi] [OUTSPI=spi]
    [ANTIREPLAYENABLED={TRUE|FALSE}] [REPLAYWINDOWSIZE={32|64|128|256}]
```

saspec-id: SA スペック番号 (0～255)

key-id: 鍵番号 (0～65535)

spi: SPI 値 (0～4294967295)。ただし、0～255 は使用すべきでない)

解説

SA スペックを作成する。

SA スペックは IPsec 通信の仕様 (パケットに適用する処理) を定義するもので、SA の動作モード (トンネル、トランスポート)、鍵管理方式 (手動、自動)、処理/プロトコル (暗号化・認証/ESP、認証/AH、圧縮/IPComp)、使用アルゴリズム (DES、MD5、SHA など)、SPI (手動設定の場合) などのパラメータを設定する。

パラメーター

SASPECIFICATION SA スペック番号

KEYMANAGEMENT 鍵管理方式。手動設定 (MANUAL) が自動設定 (ISAKMP) から選択する。

PROTOCOL IPsec プロトコル。ESP (暗号化と認証)、AH (認証)、COMP (IPComp 圧縮) から選択する。個々の SA スペックでは 1 つしかプロトコルを指定できないが、実際に IPsec 通信の設定を行うときは、SA スペックの組み合わせを「SA バンドルスペック」として指定する

MODE SA の動作モード。TUNNEL (トンネルモード) と TRANSPORT (トランスポートモード) がある。省略時は TUNNEL

COMPALGORITHM 圧縮アルゴリズム。選択肢は LZS のみだが、PROTOCOL に COMP を指定したときは必須

ENCALGORITHM 暗号化アルゴリズム。PROTOCOL に ESP を指定した場合の必須パラメーター。通常は DES (56 ビット DES) か 3DESOUTER (168 ビット 3DES) を指定する。NULL (NULL 暗号化アルゴリズム) は、ESP の認証機能だけを使いたいときやデバッグを行うときに指定する。ENCALGORITHM と HASHALGORITHM の両方に NULL を指定することはできない

ENCKEY 暗号鍵番号。PROTOCOL に ESP を指定し、KEYMANAGEMENT に MANUAL を指定した場合にのみ有効 (かつ必須)

HASHALGORITHM メッセージ認証用のハッシュアルゴリズム。PROTOCOL に AH か ESP を指定した場合の必須パラメーター。NULL は ESP の暗号化機能だけを扱い、認証機能を使わない場合に指

定する。ENCALGORITHM と HASHALGORITHM の両方に NULL を指定することはできない
HASHKEY 認証鍵番号。PROTOCOL に AH か ESP を指定し、KEYMANAGEMENT に MANUAL
 を指定した場合にのみ有効（かつ必須）

INSPI 内向きトラフィックの SPI（Security Parameter Index）値。PROTOCOL に AH か ESP を指定
 し、KEYMANAGEMENT に MANUAL を指定した場合にのみ必要

OUTSPI 外向きトラフィックの SPI（Security Parameter Index）値。PROTOCOL に AH か ESP を指
 定し、KEYMANAGEMENT に MANUAL を指定した場合にのみ必要

ANTIREPLAYENABLED リプレイ防止機能の有効・無効。PROTOCOL に COMP を指定した場合、お
 よび、手動鍵管理を使う場合は無効。デフォルトは FALSE

REPLAYWINDOWSIZE リプレイ防止ウィンドウサイズ。デフォルトは 32 パケット。PROTOCOL に
 COMP を指定した場合、および、KEYMANAGEMENT に MANUAL を指定した場合は無効

例

手動鍵管理用の SA スペック「1」を作成する。この SA では、トンネルモード ESP による暗号化と認証
 を行う。暗号化アルゴリズムには DES（鍵番号「1」）を、認証アルゴリズムには SHA（鍵番号「2」）を用い、
 SPI は内向きが 1000、外向きが 1001 とする。

```
CREATE IPSEC SASPEC=1 KEYMAN=MANUAL PROT=ESP ENCALG=DES ENCKEY=1
  HASHALG=SHA HASHKEY=2 INSPI=1000 OUTSPI=1001
```

自動鍵管理用の SA スペック「2」を作成する。この SA では、トンネルモード ESP による暗号化と認証
 を行う。暗号化アルゴリズムには DES を、認証用のハッシュアルゴリズムには SHA を用いる。暗号・認証
 鍵と SPI 値は、ISAKMP/IKE のネゴシエーションによって自動的に管理するため指定しない

```
CREATE IPSEC SASPEC=2 KEYMAN=ISAKMP PROT=ESP ENCALG=DES HASHALG=SHA
```

ESP のデバッグを行うため、実際には暗号化を行わない NULL 暗号化アルゴリズムを使用する。

```
CREATE IPSEC SASPEC=3 KEYMAN=ISAKMP PROT=ESP ENCALG=NULL HASHALG=SHA
```

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）また
 は暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DESTROY IPSEC SASPECIFICATION（51 ページ）

SET IPSEC SASPECIFICATION（81 ページ）

SHOW IPSEC SASPECIFICATION（111 ページ）

CREATE ISAKMP POLICY

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
CREATE ISAKMP POLICY=policy PEER={ipadd|ANY} [AUTHTYPE={PRESHARED|RSASIG|
RSAENCR}] [DHEXPONENTLENGTH=160..1023] [ENCALG={DES|3DES|OUTER}]
[EXPIRYKBYTES=1..1000] [EXPIRYSECONDS=600..31449600] [GROUP={0|1|2}]
[HASHALG={SHA|MD5}] [HEARTBEATMODE={BOTH|NONE|RECEIVE|SEND}]
[HYBRIDXAUTH={ON|OFF|TRUE|FALSE}] [KEY=0..65535] [LOCALID={ipadd|
domain-name|userdomainname|dist-name}] [LOCALRSAKEY=0..65535]
[MODE={MAIN|AGGRESSIVE}] [MSGRETRYLIMIT=0..1024] [MSGTIMEOUT=1..86400]
[PHASE2XCHGLIMIT={NONE|1..1024}] [POLICYFILENAME=filename]
[PRENEGOTIATE={ON|OFF|TRUE|FALSE}] [REMOTEID={ipadd|domain-name|
userdomainname|dist-name}] [SENDDELETES={ON|OFF|TRUE|FALSE}]
[SENDNOTIFY={ON|OFF|TRUE|FALSE}] [SENDIDALWAYS={ON|OFF|TRUE|FALSE}]
[SETCOMMITBIT={ON|OFF|TRUE|FALSE}] [SRCINTERFACE=interface]
[XAUTH={CLIENT|SERVER|NONE}] [XAUTHNAME=username]
[XAUTHPASSWORD=password] [XAUTHTYPE={GENERIC|RADIUS}]
```

policy: ISAKMP ポリシー名 (1~24 文字)

ipadd: IP アドレス

domain-name: ドメイン名

userdomainname: ユーザー名付きドメイン名 (user@foo.bar.xxx の形式)

dist-name: X.500 識別名 (DN) ("cn=myname,o=myorg,c=jp" の形式)

filename: ファイル名 (拡張子は.scp)

interface: IP インターフェース名 (eth0、ppp0 など)

username: ユーザー名 (1~64 文字)

password: パスワード (1~64 文字。大文字小文字を区別する)

解説

ISAKMP ポリシーを作成する。

ISAKMP ポリシーでは、ISAKMP メッセージの交換相手 (ISAKMP ピア) や使用する暗号アルゴリズムなど、ISAKMP/IKE に関する各種設定パラメーターを定義する。

ISAKMP では始動者 (ネゴシエーションを開始する側) と応答者の区別がある。

パラメーター

POLICY ISAKMP ポリシー名

PEER ISAKMP の通信相手 (ISAKMP ピア) の IP アドレスを指定する。IP アドレスを指定した場合は、始動者、応答者のどちら側にもなりうる。一方、ANY (どの相手からでも接続を受け入れる) を指定したポリシーでは必ず応答者側 (受け入れ専用) になる。

AUTHTYPE ISAKMP ピアの認証方式。PRESHARED（事前共有鍵）、RSASIG（RSA デジタル署名）、RSAENCR（RSA 公開鍵暗号）から選択する。デフォルトは PRESHARED。

DHEXPONENTLENGTH Diffie-Hellman 鍵交換アルゴリズムにおいて、各当事者が生成する乱数（ $g^a \bmod p$ における a ）の長さ（ビット）。値が大きいほど生成した鍵の安全性が高まるが、鍵の交換に時間がかかるようになる。Oakley グループ 0、1、2 いずれの場合も最小値は 160 ビット。デフォルト値も同じく 160 ビット。最大値はグループによって異なり、グループ 0 は 511 ビット、グループ 1 は 767 ビット、グループ 2 は 1023 ビット。

ENCALG ISAKMP メッセージの暗号化アルゴリズム。デフォルトは DES。

EXPIRYKBYTES ISAKMP SA の有効期限（Kbyte）。通信データ量が指定量に達すると、ISAKMP SA は再ネゴシエートされる。デフォルトは NONE（無期限）。

EXPIRYSECONDS ISAKMP SA の有効期限（秒）。SA 作成後、指定時間が経過すると、ISAKMP SA は再ネゴシエートされる。デフォルトは 86400（24 時間）。

GROUP 鍵交換時に用いる Diffie-Hellman（Oakley）グループを指定する。グループ 0（512 ビット MODP）、グループ 1（768 ビット MODP）、グループ 2（1024 ビット MODP）から選択する。デフォルトはグループ 1。

HASHALG ISAKMP メッセージの認証用ハッシュアルゴリズム。デフォルトは SHA。

HEARTBEATMODE ISAKMP ハートビートを使用するかどうか。ISAKMP ハートビートは、ルーター間の通信が途絶えたときに古い SA 情報が残らないようにする本製品の独自機能。他社製品との互換性はない。SEND を指定した場合は、20 秒間隔でハートビートメッセージを送信する。RECEIVE を指定した場合は、ハートビートメッセージの受信だけを行う。受信側は、3 回連続してハートビートを受信できなかった場合は通信が不可能になったものとみなして、対向ルーターとの間に張られた SA をすべて削除する。BOTH を指定したときは送信と受信の両方を行う。NONE はハートビートメッセージを使用しないことを示す。デフォルトは NONE。

HYBRIDXAUTH ハイブリッド型の拡張認証（XAUTH）を使用するかどうか。AUTHTYPE に RSASIG を指定した場合にのみ有効。デフォルトは OFF。

KEY ISAKMP ピアの認証に用いる鍵の番号を指定する。事前共有鍵（PRESHARED）方式の場合は各ピア共通の GENERAL 鍵（必須）を、デジタル署名（RSASIG）方式の場合は ISAKMP ピアの RSA 公開鍵を指定する。無指定の場合は、ISAKMP メッセージで相手の公開鍵証明書を要求し、CA 証明書を使って鍵の正当性を検証する。公開鍵暗号（RSAENCR）方式の場合は、ISAKMP ピアの RSA 公開鍵を指定する。無指定の場合は、ISAKMP ピアの IP アドレス（PEER）を元に ENCO モジュールの鍵データベースが検索される。

LOCALID ISAKMP フェーズ 1 において、相手に送信する ID ペイロードの内容（自分の ID 情報）を指定する。IP アドレス（例：172.16.10.5）、ドメイン名（例：bar.mydomain.net）、ユーザー名付きドメイン名（例：joger@bar.mydomain.net）、X.500 識別名（例："cn=joge,o=ournet,c=jp"）の 4 形式が使用できる。デフォルトでは、ISAKMP パケットの始点アドレスが ID として使われる。また、相手認証にデジタル署名（RSASIG）方式を使っている場合は、SET SYSTEM DISTINGUISHEDNAME コマンドで設定したシステム識別名（DN）が使用される。このパラメーターは、おもに自分の IP アドレスが不定な場合に使う。

LOCALRSAKEY 自分の RSA 秘密鍵を指定する。相手認証にデジタル署名（RSASIG）方式か公開鍵暗号（RSAENCR）方式を使う場合の必須パラメーター。ただし、ENABLE ISAKMP コマンドの LOCALRSAKEY パラメーターでデフォルト鍵を設定している場合は省略可能。その場合、デフォルト鍵が使われる。

MODE ISAKMP フェーズ 1 で使用する IKE 交換モード。ID 情報が保護される MAIN モードと ID 情報が保護されない AGGRESSIVE モードがある。相手認証に事前共有鍵 (PRESHARED) 方式を使い、なおかつ、片側のルーターのアドレスが不定な場合は、LOCALID/REMOTEID で IP アドレス以外の ID を指定し、AGGRESSIVE モードを使う必要がある。それ以外の場合は通常 MAIN モードを使う。デフォルトは MAIN モード。

MSGRETRYLIMIT ISAKMP メッセージの再送回数。デフォルトは 5

MSGTIMEOUT ISAKMP メッセージを送信してから 1 回目の再送を行うまでの待ち時間。2 回目以降の再送待ち時間はこれよりも長くなる。デフォルトは 20 秒

PHASE2XCHGLIMIT このポリシーに基づいて確立された ISAKMP SA 上で行うことのできる IKE フェーズ 2 交換の最大数。デフォルトは NONE (制限なし)

POLICYFILENAME AT-VPN Client に送るセキュリティポリシーファイルの名前を指定する。本機能を使用するには、ENABLE ISAKMP コマンドの POLICYSERVERENABLED パラメーターに TRUE を設定する必要がある。詳細は AT-VPN Client のマニュアルを参照。

PRENEGOTIATE ルーター起動時 (正確には ENABLE ISAKMP コマンドの実行時) に IKE のネゴシエーションを行っておくかどうかを指定する。デフォルトは FALSE。

REMOTEID ISAKMP フェーズ 1 において、相手から受け取ることを期待する ID ペイロードの内容 (相手の ID 情報) を指定する。IP アドレス (例: 172.16.10.5) ドメイン名 (例: bar.mydomain.net) ユーザー名付きドメイン名 (例: joger@bar.mydomain.net) X.500 識別名 (例: "cn=joge,o=ournet,c=jp") の 4 形式が使用できる。デフォルトでは、相手から受け取った ISAKMP メッセージの始点 IP アドレスを ID 値として期待する。このパラメーターは、おもに相手ルーターの IP アドレスが不定な場合に使う。

SENDDELETES SA の削除を通知する Delete ペイロードを送信するかどうか。TRUE または ON を指定した場合、ローカル側で SA 情報が削除された場合に該当 SA がもはや有効でないことを相手ルーターに通知する。これにより、無効な SA にトラフィックが送り出されることを防止できる。デフォルトは FALSE。

SENDNOTIFY IKE のステータスやエラー情報を通知する Notify ペイロードを送信するかどうか。デフォルトは FALSE。

SENDIDALWAYS ISAKMP SA のネゴシエーション時に常に ID ペイロードを送信するかどうか。デフォルトは FALSE。

SETCOMMITBIT ISAKMP SA のネゴシエーション時に ISAKMP ヘッダーの Commit ビットをオンにするかどうか。TRUE または ON を指定した場合は、SA 確立の確認メッセージを受け取るまで、SA にトラフィックが送信されないことが保証される。デフォルトは FALSE。

SRCINTERFACE ISAKMP メッセージの始点インターフェース。指定したインターフェースに有効な IP アドレスが設定されている場合は、そのアドレスが ISAKMP メッセージの始点アドレスとして使われる。

XAUTH ISAKMP フェーズ 1 終了後に拡張認証 (XAUTH) を使用するかどうか。使用する場合はサーバー (認証する側) クライアント (認証を受ける側) のどちらになるかを指定する。SERVER 指定時は、ISAKMP ピアに対して XAUTH の認証要求を送る。CLIENT 指定時は、ISAKMP ピアからの XAUTH 認証要求を期待する。NONE は XAUTH を使わない。デフォルトは NONE。

XAUTHNAME XAUTH 使用時のユーザー名。クライアント側が指定する。

XAUTHPASSWORD XAUTH 使用時のパスワード。クライアント側が指定する。

XAUTHTYPE XAUTH 使用時の認証方式。GENERAL (ユーザー認証データベース) または RADIUS

から選択する。デフォルトは GENERIC。

例

5 つの ISAKMP ポリシーを作成する。「xauth」はすべての XAUTH ユーザーをまかなうポリシー。「dyn1」「dyn2」はアドレス不定の user1、user2 からの接続を受け入れるためのポリシー（Aggressive モードで FQDN の ID を使用）。「fix1」「fix2」はアドレス固定の相手から接続を受け入れるためのポリシー（Main モードでデフォルトの IP アドレス形式の ID を使用）。

```
CREATE ISAKMP POLICY=xauth PEER=ANY KEY=0 XAUTH=SERVER SENDN=TRUE
    SETC=TRUE
CREATE ISAKMP POLICY=dyn1 PEER=ANY KEY=1 MODE=AGGR SENDN=TRUE
    REMOTEID=user1
CREATE ISAKMP POLICY=dyn2 PEER=ANY KEY=2 MODE=AGGR SENDN=TRUE
    REMOTEID=user2
CREATE ISAKMP POLICY=fix1 PEER=1.1.1.1 KEY=11 SENDN=TRUE
CREATE ISAKMP POLICY=fix2 PEER=2.2.2.2 KEY=12 SENDN=TRUE
```

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

「PRENEGOTIATE=TRUE」を指定する場合は、ENABLE ISAKMP コマンドが実行されるときに、すでに ISAKMP ポリシーが定義されていなくてはならない。具体的には ENABLE ISAKMP コマンドより前に CREATE ISAKMP POLICY コマンドが実行されなくてはならない。設定ファイルを EDIT コマンド等で編集するときは注意すること。

関連コマンド

DESTROY ISAKMP POLICY (52 ページ)

SET ISAKMP POLICY (84 ページ)

SHOW ISAKMP POLICY (122 ページ)

DESTROY IPSEC BUNDLESPECIFICATION

カテゴリー：IPsec / SA バンドルスペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY IPSEC BUNDLESPECIFICATION=*bspec-id*

bspec-id: SA バンドルスペック番号 (0~255)

解説

SA バンドルスペックを削除する。

パラメーター

BUNDLESPECIFICATION SA バンドルスペック番号

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE IPSEC BUNDLESPECIFICATION (37 ページ)

SET IPSEC BUNDLESPECIFICATION (77 ページ)

SHOW IPSEC BUNDLESPECIFICATION (89 ページ)

DESTROY IPSEC POLICY

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY IPSEC POLICY=*policy* [SABUNDLE=*bundle-id*]

policy: IPsec ポリシー名 (1～23 文字)

bundle-id: SA バンドル番号 (0～65535)

解説

IPsec ポリシー、または、指定ポリシーに基づいて作成された SA バンドルを削除する。

IPsec ポリシーそのものを削除した場合は、同ポリシーに基づくアクティブな SA バンドルもすべて削除される。

パラメーター

POLICY IPsec ポリシー名

SABUNDLE SA バンドル番号 (SHOW IPSEC POLICY コマンドの SABUNDLE オプションで確認できる)

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE IPSEC POLICY (39 ページ)

DISABLE IPSEC POLICY DEBUG (54 ページ)

ENABLE IPSEC POLICY DEBUG (59 ページ)

SET IPSEC POLICY (78 ページ)

SHOW IPSEC POLICY (96 ページ)

DESTROY IPSEC SASPECIFICATION

カテゴリー：IPsec / SA スペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY IPSEC SASPECIFICATION=*saspec-id*

saspec-id: SA スペック番号 (0 ~ 255)

解説

SA スペックを削除する。

パラメーター

SASPECIFICATION SA スペック番号

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE IPSEC SASPECIFICATION (43 ページ)

SET IPSEC SASPECIFICATION (81 ページ)

SHOW IPSEC SASPECIFICATION (111 ページ)

DESTROY ISAKMP POLICY

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY ISAKMP POLICY=*policy*

policy: ISAKMP ポリシー名（1～24 文字）

解説

ISAKMP ポリシーを削除する。

パラメーター

POLICY ISAKMP ポリシー名

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

CREATE ISAKMP POLICY（45 ページ）

SHOW ISAKMP POLICY（122 ページ）

DISABLE IPSEC

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

DISABLE IPSEC

解説

IPsec モジュールを無効にする。

アクティブな SA バンドルはすべて削除される。IPsec ポリシーは削除されない。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE IPSEC POLICY DEBUG（54 ページ）

DISABLE ISAKMP（56 ページ）

ENABLE IPSEC（58 ページ）

ENABLE IPSEC POLICY DEBUG（59 ページ）

ENABLE ISAKMP（62 ページ）

PURGE IPSEC（72 ページ）

SHOW IPSEC（88 ページ）

DISABLE IPSEC POLICY DEBUG

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
DISABLE IPSEC POLICY={policy|ALL} DEBUG={ALL|FILTER|PACKET|TRACE}
[DIRECTION={ALL|IN|OUT}] [DISPLAY={ALL|BUFFERHEADER|DATA|IPHEADER}]
[RESULT={ALL|FAIL|PASS}] [SELECTOR={ALL|LADDRESS|LNAME|LPORT|RADDRESS|
RNAME|RPORT|TRANSPORTPROTOCOL}] [WHERE={ALL|IPSEC|PROTOCOL}]
```

policy: IPsec ポリシー名 (1～23 文字)

解説

IPsec ポリシーのデバッグオプションを無効にする。

パラメーター

POLICY IPsec ポリシー名

DEBUG 無効にするデバッグオプション。FILTER (ポリシーフィルターのデバッグ)、PACKET (IPsec パケットのデバッグ)、TRACE (トレースデバッグ)、ALL (すべて) から選択する。

DIRECTION デバッグオプションを無効にするトラフィックの向き。IN (内向き)、OUT (外向き)、BOTH (双方向) から選択する。

DISPLAY パケットデバッグ (DEBUG=PACKET) において、パケットの一部について表示を抑制したいときに指定する。ALL を指定すると、パケット表示が行われなくなる。BUFFERHEADER、DATA、IPHEADER は、それぞれバッファヘッダー、データ、IP ヘッダーの表示だけを無効にする。

RESULT フィルターデバッグ (DEBUG=FILTER) において、特定パケットのデバッグを抑制したいときに指定する。ALL を指定すると、フィルターデバッグがすべて無効になる。FAIL、PASS は、それぞれフィルターにマッチしなかったパケット、マッチしたパケットのデバッグだけを無効にする。

SELECTOR フィルターデバッグ (DEBUG=FILTER) において、特定フィルター条件 (セレクトター) についてだけデバッグを無効にしたいときに指定する。

WHERE パケットデバッグ (DEBUG=PACKET) において、特定のプロトコル処理部についてのみデバッグを無効にしたいときに指定する。IPSEC は IPsec 処理部、PROTOCOL は各 IPsec プロトコルの処理部、ALL はすべてを意味する。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

ENABLE IPSEC POLICY DEBUG (59 ページ)

SHOW IPSEC POLICY (96 ページ)

DISABLE ISAKMP

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

DISABLE ISAKMP

解説

ISAKMP モジュールを無効にする。

アクティブな ISAKMP SA はすべて削除される。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE ISAKMP DEBUG（57 ページ）

ENABLE ISAKMP（62 ページ）

ENABLE ISAKMP DEBUG（64 ページ）

SHOW ISAKMP（114 ページ）

DISABLE ISAKMP DEBUG

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

DISABLE ISAKMP DEBUG={ALL|DEFAULT|PACKET|PKT|PKTRAW|STATE|TRACE|
TRACEMORE}

解説

ISAKMP モジュールのデバッグオプションを無効にする。

パラメーター

DEBUG 無効にするデバッグオプション。STATE (ISAKMP の状態遷移デバッグ)、PACKET または PKT (ISAKMP メッセージのデバッグ)、PKTRAW (ISAKMP メッセージの 16 進ダンプ)、TRACE (ISAKMP トレースデバッグ)、TRACEMORE (ISAKMP 計算値のデバッグ)、DEFAULT (TRACE、STATE、PACKET を指定したのと同じ)、ALL (すべて) から選択する。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

DISABLE ISAKMP (56 ページ)

ENABLE ISAKMP (62 ページ)

ENABLE ISAKMP DEBUG (64 ページ)

SHOW ISAKMP (114 ページ)

ENABLE IPSEC

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

ENABLE IPSEC

解説

IPsec モジュールを有効にする。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE IPSEC（53 ページ）

DISABLE IPSEC POLICY DEBUG（54 ページ）

DISABLE ISAKMP（56 ページ）

ENABLE IPSEC POLICY DEBUG（59 ページ）

ENABLE ISAKMP（62 ページ）

PURGE IPSEC（72 ページ）

SHOW IPSEC（88 ページ）

ENABLE IPSEC POLICY DEBUG

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
ENABLE IPSEC POLICY [=policy] DEBUG={ALL|FILTER|PACKET|TRACE}
    [DIRECTION={ALL|IN|OUT}] [DISPLAY={ALL|BUFFERHEADER|DATA|IPHEADER}]
    [RESULT={ALL|FAIL|PASS}] [SELECTOR={ALL|LADDRESS|LNAME|LPORT|RADDRESS|
    RNAME|RPORT|TRANSPORTPROTOCOL}] [WHERE={ALL|IPSEC|PROTOCOL}]
```

policy: IPsec ポリシー名（1～23 文字）

解説

IPsec ポリシーのデバッグオプションを有効にする。

パラメーター

POLICY IPsec ポリシー名

DEBUG 有効にするデバッグオプション。FILTER（IPsec ポリシーによるパケットフィルタリングの過程を表示）、PACKET（IPsec パケットを 16 進ダンプ表示）、TRACE（IPsec 処理の過程をトレース）、ALL（すべて）から選択する。

DIRECTION デバッグオプションを有効にするトラフィックの向き。IN（内向き）、OUT（外向き）、BOTH（双方向）から選択する。

DISPLAY パケットデバッグ（DEBUG=PACKET）において、パケットの一部について表示を有効にしたいときに指定する。ALL を指定すると、すべての表示がオンになる。BUFFERHEADER、DATA、IPHEADER は、それぞれバッファヘッダー、データ、IP ヘッダーの表示だけを有効にする。

RESULT フィルターデバッグ（DEBUG=FILTER）において、特定パケットのデバッグを有効にしたいときに指定する。ALL を指定すると、フィルターデバッグがすべて有効になる。FAIL、PASS は、それぞれフィルターにマッチしなかったパケット、マッチしたパケットのデバッグだけを有効にする。

SELECTOR フィルターデバッグ（DEBUG=FILTER）において、特定フィルター条件（セレクター）についてだけデバッグを有効にしたいときに指定する。

WHERE パケットデバッグ（DEBUG=PACKET）において、特定のプロトコル処理部についてのみデバッグを有効にしたいときに指定する。IPSEC は IPsec 処理部、PROTOCOL は各 IPsec プロトコルの処理部、ALL はすべてを意味する。

入力・出力・画面例

```
SecOff > ena ipsec policy=vpn debug=filter

Info (181057): IPSEC Policy Debugging has been enabled.
```

```

SecOff >
IPSEC: filt: pass: laddr: pol vpn
           pol 192.168.20.0:255.255.255.0, pkt 192.168.20.100

IPSEC: filt: pass: raddr: pol vpn
           pol 192.168.1.0:255.255.255.0, pkt 192.168.1.2

IPSEC: filt: pass: laddr: sa 2
           sa 192.168.20.0:255.255.255.0, pkt 192.168.20.100

IPSEC: filt: pass: raddr: sa 2
           sa 192.168.1.0:255.255.255.0, pkt 192.168.1.2

SecOff > ena ipsec policy=vpn debug=packet

Info (181057): IPSEC Policy Debugging has been enabled.

SecOff >
IPSEC vpn: 2: OUT: pre processing:
IP: 45000028eb1040002006d908c0a81464c0a80102
TCP: 0429005005b7e65c01faee4c5004000038560000
data:

IPSEC vpn: 2: OUT: post processing:
IP: 450000604b7f00004032fa573f0c42ef3d737527
ESP: 14f45fa300000b09:35d26e02458706623d9aa9bf
data: 9fcd18d0a34ffeeeb8b0f574ddeaa820f8ba0db36cd7a9fc0254f08215e2aa7ecdb34688
      6193f17d39cc7f096276238bf262b668920b51c535d26e02458706623d9aa9bf

SecOff > ena ipsec policy=vpn debug=trace

Info (181057): IPSEC Policy Debugging has been enabled.

SecOff >
IPSEC vpn: 2: OUT: pre processing:
IP: 4500002cf81040002006cc04c0a81464c0a80102
TCP: 042c005005b9c354000000006002200013e60000
data: 020405b4

IPSEC vpn: 2: OUT: post processing:
IP: 450000604b8000004032fa563f0c42ef3d737527
ESP: 14f45fa300000b0a:303cd3682ca0d4724d415643
data: f6bdc7fc7a25cbb885eb3461ce36cda7bbf752aa3298a3b5ef1f3aae0d8b94aa19d769f5
      95fc677f693c2b0ecfe13a5feae75b52430aa46d303cd3682ca0d4724d415643

SecOff >
IPSEC vpn: 2: IN: pre processing:
IP: 450000605ae800003732f3ee3d7375273f0c42ef
ESP: 52d700ff00000c8c:29109cc701bee3a76460a2eb

```

```
data: 993a2918084608c51648755a8f6ebd12d68f806a169d4c243a04c0741d50a3ab52493dcd  
      069d1ec17a17349b9ec9f6c6bb739a39b576298129109cc701bee3a76460a2eb  
  
IPSEC vpn: 2: IN: post processing:  
IP:      4500002c5ae500003f068a30c0a80102c0a81464  
TCP:     0050042cf254a5a005b9c355601204009b7b0000  
data: 02040218
```

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE IPSEC POLICY DEBUG（54 ページ）

SHOW IPSEC POLICY（96 ページ）

ENABLE ISAKMP

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

ENABLE ISAKMP [LOCALRSAKEY=*key-id*] [POLICYSERVERENABLED={TRUE|FALSE}]
[POLICYFILENAME=*filename*] [UDPSPORT=*port*]

filename: ファイル名（拡張子は.scp）

key-id: 鍵番号（0～65535）

port: UDP ポート番号（1～65535）

解説

ISAKMP モジュールを有効にする。

PRENEGOTIATE=TRUE の ISAKMP ポリシーが存在する場合は、有効にすると同時にフェーズ 1 のネゴシエーションが開始される。

パラメーター

LOCALRSAKEY 自分の RSA 秘密鍵を指定する。ISAKMP の相手認証にデジタル署名（RSASIG）方式か公開鍵暗号（RSAENCR）方式を使っている場合、ここで指定した鍵がデフォルト鍵となる。

POLICYSERVERENABLED セキュリティポリシーサーバー機能を有効にするかどうか。本機能は、AT-VPN Client からの要求に対し、POLICYFILENAME で指定したポリシーファイルを送信する機能。詳細は AT-VPN Client のマニュアルを参照のこと。

POLICYFILENAME セキュリティポリシーサーバーとしての動作時に、AT-VPN Client に送信するポリシーファイルの名前。ISKAMP ポリシーの POLICYFILENAME パラメーターでファイル名を指定している場合は、そちらが優先的に使用される。

UDPSPORT ISAKMP メッセージの送受信に使用する UDP ポート。デフォルトは 500。

備考・注意事項

PRENEGOTIATE=TRUE の ISAKMP ポリシーがある場合、設定ファイル（*.cfg）中では ENABLE ISAKMP コマンドの前に CREATE ISAKMP POLICY コマンドが来るようにすること。言い換えると、ENABLE ISAKMP コマンドが最後の ISAKMP 関連コマンドになるようにすればよい。

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE ISAKMP（56 ページ）

DISABLE ISAKMP DEBUG（57 ページ）

ENABLE ISAKMP DEBUG (64 ページ)

SHOW ISAKMP (114 ページ)

ENABLE ISAKMP DEBUG

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

ENABLE ISAKMP DEBUG={**ALL**|**DEFAULT**|**PACKET**|**PKT**|**PKTRAW**|**STATE**|**TRACE**|**TRACEMORE**}

解説

ISAKMP モジュールのデバッグオプションを有効にする。

パラメーター

DEBUG 有効にするデバッグオプション。STATE (ISAKMP の状態遷移を表示)、PACKET または PKT (ISAKMP メッセージをデコードして表示)、PKTRAW (ISAKMP メッセージを 16 進ダンプで表示)、TRACE (ISAKMP の処理過程をトレース)、TRACEMORE (ISAKMP の処理過程をより詳細にトレース)、DEFAULT (TRACE、STATE、PACKET を指定したのと同じ)、ALL (すべて) から選択する。

入力・出力・画面例

```
SecOff > enable isakmp debug=packet

SecOff > ISAKMP Tx Message
  Cookie's:    f7f11f139bcf2de0:0000000000000000
  Xchg Type:   IDPROT(2)  Ver: 10  Flags: 00
  MessageID:   00000000   Total Length: 84
  Payload #:   0   Length: 56   Type: Security Association (SA)
    DOI: IPSEC(0)  Situation: 00000001
    Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
      Transform#: 1
        Transform Id ..... IKE(1)
        Encryption Algorithm..... DES(1)
        Authentication Algorithm..... SHA(2)
        Authentication Method..... PRESERVED(1)
        Group Description..... 768(1)
        Group Type..... MODP
        Expiry Seconds..... 86400

SecOff > ISAKMP Rx Message
  Cookie's:    f7f11f139bcf2de0:599d82efe4a01228
  Xchg Type:   IDPROT(2)  Ver: 10  Flags: 00
  MessageID:   00000000   Total Length: 84
  Payload #:   0   Length: 56   Type: Security Association (SA)
```



```

DOI: IPSEC(0)  Situation: 00000001
Proposal#: 1  Protocol: ISAKMP(1)  #Trans: 1  SPI:
Transform#: 1
  Transform Id ..... IKE(1)
  Encryption Algorithm..... DES(1)
  Authentication Algorithm..... SHA(2)
  Authentication Method..... PRESHARED(1)
  Group Description..... 768(1)
  Group Type..... MODP
  Expiry Seconds..... 86400
ISAKMP Tx Message
  Cookie's:   f7f11f139bcf2de0:599d82efe4a01228
  Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
  MessageID:  00000000   Total Length: 152
  Payload #:   0   Length: 100   Type: Key Exchange (KE)
    2d df 75 56 ed ee 00 6b 11 a6 e0 47 08 b3 77 a0 53 19 68 7f
    34 f5 58 ea b7 a3 b1 0b 32 df 7d 22 85 ae ce 21 5d 80 d1 30
    52 7a c4 fb 74 18 26 d7 13 ad 1b 97 83 fc 81 ea 1b 7c a2 33
    86 3a ce 01 fe f6 50 43 c7 dd 4c f6 78 ce 2a a0 e6 af f8 93
    ee 4e cb d6 fd 78 94 c6 a1 9e 4f 15 b1 d6 21 ff
  Payload #:   1   Length: 24   Type: Nonce (NONCE)
    06 b3 a8 ce 3e 3a 04 d6 d8 16 7b 47 08 50 c9 34 9d 3f 51 82

SecOff > ISAKMP Rx Message
  Cookie's:   f7f11f139bcf2de0:599d82efe4a01228
  Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
  MessageID:  00000000   Total Length: 152
  Payload #:   0   Length: 100   Type: Key Exchange (KE)
    bb 81 9f f5 5c 89 4f 41 39 a8 92 74 1c 4b 2f 27 8b 6d 97 35
    42 45 da 93 78 0c 48 81 2a 71 ba 1b 85 cf 9a 9c ed 96 2d e6
    8e 05 c3 fe ca be 2f 95 c0 3c fa cf c5 1d 2b 28 87 71 21 75
    86 79 ad fa c0 1f 3b 0d 87 e0 0c 7d 92 f4 f7 a3 f8 0a fc 5f
    d6 fc d4 b9 05 ae c3 35 f1 27 78 b6 1e 88 98 8a
  Payload #:   1   Length: 24   Type: Nonce (NONCE)
    65 ab 76 d1 57 db 46 36 d8 e3 e0 38 0f 2d d1 d1 c3 5a d9 db

ISAKMP Tx Message
  Cookie's:   f7f11f139bcf2de0:599d82efe4a01228
  Xchg Type:  IDPROT(2)  Ver: 10  Flags: 00
  MessageID:  00000000   Total Length: 94
  Payload #:   0   Length: 14   Type: Identification (ID)
    Type: FQDN  ProtocolId: 0  Port: 0
    Value: client
  Payload #:   1   Length: 24   Type: Hash (HASH)
    19 96 21 3d 14 4f f1 3f 16 bd 3a ca 2c 8c c3 7c 03 e8 52 f2
  Payload #:   2   Length: 28   Type: Notification (N)
    00 00 00 01 01 10 60 02 f7 f1 1f 13 9b cf 2d e0 59 9d 82 ef
    e4 a0 12 28

SecOff > ISAKMP Rx Message (decrypted)
  Cookie's:   f7f11f139bcf2de0:599d82efe4a01228
  Xchg Type:  IDPROT(2)  Ver: 10  Flags: 01

```

```

MessageID: 00000000   Total Length: 92
Payload #: 0   Length: 12   Type: Identification (ID)
    Type: IPV4_ADDR   ProtocolId: 0   Port: 0
    Value: 1.1.1.1
Payload #: 1   Length: 24   Type: Hash (HASH)
    79 33 1f c5 75 4b 8b 83 0f e9 bf b7 35 81 40 77 4c 34 3d 9a
Payload #: 2   Length: 28   Type: Notification (N)
    00 00 00 01 01 10 60 02 f7 f1 1f 13 9b cf 2d e0 59 9d 82 ef
    e4 a0 12 28
ISAKMP Tx Message
Cookie's:   f7f11f139bcf2de0:599d82efe4a01228
Xchg Type:  QUICK(32)   Ver: 10   Flags: 00
MessageID:  7736489b   Total Length: 148
Payload #: 0   Length: 24   Type: Hash (HASH)
    aa 05 0b be 05 fb 74 2e 93 34 53 d8 fb 39 e0 1e a5 8f 20 42
Payload #: 1   Length: 40   Type: Security Association (SA)
    DOI: IPSEC(0)   Situation: 00000001
    Proposal#: 1   Protocol: ESP(3)   #Trans: 1   SPI: 3f854d43
    Transform#: 1
        Transform Id ..... DES(2)
        Group Description ..... MODP768(1)
        Encapsulation Mode ..... TUNNEL(1)
        Authentication Algorithm ..... SHA(2)
Payload #: 2   Length: 24   Type: Nonce (NONCE)
    b6 6b 17 23 d6 f4 04 9d 60 9d a9 84 b9 29 99 d6 5c 05 79 e9
Payload #: 3   Length: 16   Type: Identification (ID)
    Type: IPV4_ADDR_SUBNET   ProtocolId: 0   Port: 0
    Value: 192.168.20.0:255.255.255.0
Payload #: 4   Length: 16   Type: Identification (ID)
    Type: IPV4_ADDR_SUBNET   ProtocolId: 0   Port: 0
    Value: 192.168.1.0:255.255.255.0

SecOff > ISAKMP Rx Message (decrypted)
Cookie's:   f7f11f139bcf2de0:599d82efe4a01228
Xchg Type:  QUICK(32)   Ver: 10   Flags: 01
MessageID:  7736489b   Total Length: 148
Payload #: 0   Length: 24   Type: Hash (HASH)
    71 d5 87 4e 5c ec 75 fd 1f fc 0c 91 27 a0 70 79 5c 17 9c f7
Payload #: 1   Length: 40   Type: Security Association (SA)
    DOI: IPSEC(0)   Situation: 00000001
    Proposal#: 1   Protocol: ESP(3)   #Trans: 1   SPI: 58dfdda5
    Transform#: 1
        Transform Id ..... DES(2)
        Group Description ..... MODP768(1)
        Encapsulation Mode ..... TUNNEL(1)
        Authentication Algorithm ..... SHA(2)
Payload #: 2   Length: 24   Type: Nonce (NONCE)
    e2 bc 6f 0b 49 00 55 70 d2 0d f5 99 fe cc 95 af f9 4b 16 4c
Payload #: 3   Length: 16   Type: Identification (ID)
    Type: IPV4_ADDR_SUBNET   ProtocolId: 0   Port: 0
    Value: 192.168.20.0:255.255.255.0

```

```

    Payload #: 4 Length: 16 Type: Identification (ID)
      Type: IPV4_ADDR_SUBNET ProtocolId: 0 Port: 0
      Value: 192.168.1.0:255.255.255.0
ISAKMP Tx Message
  Cookie's: f7f11f139bcf2de0:599d82efe4a01228
  Xchg Type: QUICK(32) Ver: 10 Flags: 00
  MessageID: 7736489b Total Length: 52
  Payload #: 0 Length: 24 Type: Hash (HASH)
    79 2f 7b ec f1 02 d7 0d 49 47 cc 04 ce 7b 95 d4 03 47 da 21

SecOff > enable isakmp debug=state

Info (182057): ISAKMP Debugging has been enabled.

SecOff > ISAKMP MAIN exchange 11: New State: IDLE

ISAKMP MAIN exchange 11: New State: SASENT

SecOff > ISAKMP MAIN exchange 11: New State: SARECV

ISAKMP MAIN exchange 11: New State: KESENT

SecOff > ISAKMP MAIN exchange 11: New State: KERECV

ISAKMP MAIN exchange 11: New State: AUTHSENT

SecOff > ISAKMP MAIN exchange 11: New State: AUTHRECV

ISAKMP MAIN exchange 11: New State: UP

ISAKMP QUICK exchange 12: New State: SENDING_HASH_SA_NONCE

SecOff >
ISAKMP QUICK exchange 12: New State: RECEIVING_MESSAGE

ISAKMP QUICK exchange 12: New State: SENDING_HASH
ISAKMP QUICK exchange 12: New State: DONE

SecOff > enable isakmp debug=trace

Info (182057): ISAKMP Debugging has been enabled.

SecOff > sh pISAKMP: acquire - Create Phase 1 Exchange
ISAKMP MAIN: INIT: xchg 13: Started with peer 1.1.1.1
ISAKMP CORE: Aquire: equivalent acquire request in progress

```

```

SecOff > ISAKMP MAIN: INIT: xchg 13: Ni l=20 v=baa95ac53c8b47a16cff9a81fd3df98bf
34c9729
ISAKMP MAIN: INIT: xchg 13: Nr l=20 v=ed3b6400668c47c8361f853e998ff0b4d20a24d5
ISAKMP MAIN: INIT: xchg 13: COOKIE_I l=8 v=b8230e5ecac0212c
ISAKMP MAIN: INIT: xchg 13: COOKIE_R l=8 v=af3b896d8b1b2b76
ISAKMP MAIN: INIT: xchg 13: Key l=8 v=686f6765686f6765
ISAKMP MAIN: INIT: xchg 13: EncKey l=8 v=f20facb52abb3e08
ISAKMP MAIN: INIT: xchg 13: IV l=8 v=bdf0e35f5bb0459f

SecOff > ISAKMP InfoProcess: xchg 13: Rx Notification Message - DOI
ISAKMP MAIN: INIT: xchg 13: RemoteID=IPv4:1.1.1.1
ISAKMP CORE: Exchange 13 done

ISAKMP QUICK: INIT: xchg 14: Started with peer 1.1.1.1
ISAKMP QUICK: INIT: xchg 14: COOKIE_I l=8 v=b8230e5ecac0212c
ISAKMP QUICK: INIT: xchg 14: COOKIE_R l=8 v=af3b896d8b1b2b76
ISAKMP QUICK: INIT: xchg 14: MessageID=57339a70
ISAKMP QUICK: INIT: xchg 14: IV l=8 v=a73675e6799eef15

ISAKMP QI 14: HASH1: ID Payload Created

SecOff > ISAKMP QUICK: INIT: xchg 14: rx msg 1: start
ISAKMP QUICK: INIT: xchg 14: rx msg 1: prop policy done
ISAKMP QUICK: INIT: xchg 14: rx msg 1: TRAN 0,1 attributes good
ISAKMP QUICK: INIT: xchg 14: rx msg 1: TRAN 0,1 match
ISAKMP QUICK: INIT: xchg 14: rx msg 1: prop 0 match
ISAKMP QUICK: INIT: xchg 14: rx msg 1: All proposals matched: (lpn 1)
ISAKMP QUICK: INIT: xchg 14: rx msg 1: payloads good:
ISAKMP QUICK: INIT: xchg 14: rx msg 1: good
ISAKMP CORE: Exchange 14 done

SecOff > enable isakmp debug=tracemore

Info (182057): ISAKMP Debugging has been enabled.

SecOff > ISAKMP MAIN: INIT: xchg 15: Started with peer 1.1.1.1

ISAKMP: acquire - Queue the acquire struct

ISAKMP: acquire - Queue the acquire struct

SecOff > ISAKMP MAIN: INIT: xchg 15: x l=20 v=dee78c5e6d57a2b091e805d48b5cf4d7b6
2a6e5d
ISAKMP MAIN: INIT: xchg 15: g^x l=96 v=fa431d749ddb3ebada8ef569f9da7960464a8ff7f
59465ee024e0bb130c77f468ad275cbbcb62314bd0184a5f0ad9f170894ab56f666510df2bb7946cf
07167605fbaf4634ba8b6ebc7378c1e06c5e9ad5000ffefc8d27904fac1a9131b29b09e
ISAKMP MAIN: INIT: xchg 15: g^y l=96 v=4bafa551598eb94183a7fdbe7deec732404b6330b
0bfc9ee9ad4abb63bfd58f97d3c73320882e33984a4146fad9e29f3e0d17262567f7fe612dfea2b9
7662808a3ef3e868f0482e73ff550e96a39f33ebc9c4a929080529536aa569bb19a8f08

```

```

ISAKMP MAIN: INIT: xchg 15: g^xy l=96 v=8c8a03e1564abad8868b40fc7d5bca62a6a79950
405d296d9523d061bfd866dala2ef286aac69939e6f1516fc5620ee2751420b88a64f86de0041875
feb0ed62a0328a1e2fd7d90e01b42d0c3d315ece5d0167811b3d77dea899b8378edb2a01
ISAKMP MAIN: INIT: xchg 15: Ni l=20 v=8e1eade9adda0c95289025ad0b322520f7c00a93
ISAKMP MAIN: INIT: xchg 15: Nr l=20 v=16e83cf248d4c890bee7ef266cfb82788d83557a
ISAKMP MAIN: INIT: xchg 15: COOKIE_I l=8 v=c7fb026ba87dc835
ISAKMP MAIN: INIT: xchg 15: COOKIE_R l=8 v=649adcdb744a7018
ISAKMP MAIN: INIT: xchg 15: Key l=8 v=686f6765686f6765
ISAKMP MAIN: INIT: xchg 15: SKEYID l=20 v=073f3d19abde74d9a3ab8584c99dc084c97929
e9
ISAKMP MAIN: INIT: xchg 15: SKEYID_d l=20 v=dbdaf57885e0e76e580cf4e696c9c07312c9
3569
ISAKMP MAIN: INIT: xchg 15: SKEYID_a l=20 v=6e6525ff8853e3239c374c9e0b604956e420
84eb
ISAKMP MAIN: INIT: xchg 15: SKEYID_e l=20 v=5483967a2001308d33adb5ff26a6a10efd48
6c21
ISAKMP MAIN: INIT: xchg 15: EncKey l=8 v=5483967a2001308d
ISAKMP MAIN: INIT: xchg 15: IV l=8 v=a05ded8713462c0c
ISAKMP MAIN: INIT: xchg 15: Hi l=20 v=3d202c887fb67a69bb5e8851606a5f9d7184faf7

SecOff > ISAKMP MAIN: INIT: xchg 15: RemoteID=IPv4:61.115.117.39
ISAKMP MAIN: INIT: xchg 15: Hr l=20 v=77c2972f612e22418e867a30dbdbeda4c729edb6
ISAKMP DOI: IPSEC: Exchange IDs from selectors:
  IDi: type          IPV4_ADDR_SUBNET
       protocol Id    0
       port           0
       data            c0a81400ffffff00
  IDr: type          IPV4_ADDR_SUBNET
       protocol Id    0
       port           0
       data            c0a80100ffffff00
ISAKMP DOI: IPSEC: Aquire Info -> Local Policy
  number of proposals 1
  proposal 0: # 1, protId 3, #transforms 1
    transform 0: # 1, id 2, sas 1
      expiry: b 0-4294967295, s 0-28800
      gr 1, mode 1, auth 2
ISAKMP QUICK: INIT: xchg 16: Started with peer 1.1.1.1
ISAKMP DOI: IPSEC: Exchange IDs not default:
  initiatorAddress    63.12.66.122
  IDi: type          IPV4_ADDR_SUBNET
       protocol Id    0
       port           0
       data            c0a81400ffffff00
  responderAddress    1.1.1.1
  IDr: type          IPV4_ADDR_SUBNET
       protocol Id    0
       port           0
       data            c0a80100ffffff00

ISAKMP QI 16: HASH1: 008390d4 100

```

```

204ebb1d0a00002800000001000000010000001c01030401157652f200000010
01020000800400018005000205000018099f36cc5dfa4c00c3c97a5f00ad334f
7eae9c070500001004000000c0a81400ffffff000000001004000000c0a80100
ffffff00

ISAKMP QI 16: HASH1: result f21b2f7aa43130b98db2e8a3eccc6921855d10dd

SecOff > ISAKMP QUICK: INIT: xchg 16: rx msg 1: start
ISAKMP QUICK: INIT: xchg 16: rx msg 1: prop policy done
ISAKMP QUICK: INIT: xchg 16: rx msg 1: TRAN 0,1 attributes good
ISAKMP QUICK: INIT: xchg 16: rx msg 1: TRAN 0,1 match
ISAKMP QUICK: INIT: xchg 16: rx msg 1: prop 0 match
ISAKMP QUICK: INIT: xchg 16: rx msg 1: All proposals matched: (lpn 1)
ISAKMP QUICK: INIT: xchg 16: rx msg 1: payloads good:
ISAKMP QUICK: INIT: xchg 16: rx msg 1: good

ISAKMP QI 16: HASH2: 009c58d4 120
204ebb1d099f36cc5dfa4c00c3c97a5f00ad334f7eae9c070a00002800000001
0000000100000001c01030401227095c8000000010010200008004000180050002
05000018a095527f8c5274284d602fbc4f865fc1ae4490ea0500001004000000
c0a81400ffffff000000001004000000c0a80100ffffff00

ISAKMP QI 16: HASH2: result 52016de8012ee5ec2a74f60e6d571bcae625b8fe

ISAKMP QI 16: HASH INK1: 009e40d4 45
03157652f2099f36cc5dfa4c00c3c97a5f00ad334f7eae9c07a095527f8c5274
284d602fbc4f865fc1ae4490ea

ISAKMP QI 16: HASH INK1: result 95e9b959f1e819bc12e896bf227eb78a184f8c6a

ISAKMP QI 16: HASH OUTK1: 009e40d4 45
03227095c8099f36cc5dfa4c00c3c97a5f00ad334f7eae9c07a095527f8c5274
284d602fbc4f865fc1ae4490ea

ISAKMP QI 16: HASH OUTK1: result 8303f4ba30e24de1dac0b835b11046fbb5f0f85f

ISAKMP QI 16: HASH INK2: 009e40c0 65
95e9b959f1e819bc12e896bf227eb78a184f8c6a03157652f2099f36cc5dfa4c
00c3c97a5f00ad334f7eae9c07a095527f8c5274284d602fbc4f865fc1ae4490
ea

ISAKMP QI 16: HASH INK1: result 95e9b959f1e819bc12e896bf227eb78a184f8c6a

ISAKMP QI 16: HASH OUTK1: 009e40c0 65
8303f4ba30e24de1dac0b835b11046fbb5f0f85f03227095c8099f36cc5dfa4c
00c3c97a5f00ad334f7eae9c07a095527f8c5274284d602fbc4f865fc1ae4490
ea

ISAKMP QI 16: HASH OUTK2: result 52112530c1000cc247cdea99096bad13f19e25c9

ISAKMP QI 16: HASH3: 0080b0d4 45

```

```
00204ebb1d099f36cc5dfa4c00c3c97a5f00ad334f7eae9c07a095527f8c5274
284d602fbc4f865fc1ae4490ea

ISAKMP QI 16: HASH3: result 14014fd9c3a2749b6c65a0b42f0c558aede913d2
```

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE ISAKMP（56 ページ）

DISABLE ISAKMP DEBUG（57 ページ）

ENABLE ISAKMP（62 ページ）

SHOW ISAKMP（114 ページ）

PURGE IPSEC

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

PURGE IPSEC

解説

IPsec の設定情報をすべて削除する。

備考・注意事項

ランタイムメモリー上にある IPsec 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DESTROY IPSEC POLICY（50 ページ）

DISABLE IPSEC（53 ページ）

ENABLE IPSEC（58 ページ）

SHOW IPSEC（88 ページ）

RESET IPSEC COUNTER

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

RESET IPSEC COUNTER [= {AH|ALG|COMP|ESP|MAIN|SAD|SETUP|SPD}]

解説

IPsec 関連の統計カウンターをクリアする。

パラメーター

COUNTER クリアするカウンターのカテゴリーを指定する。省略時および ALL を指定した場合はすべてのカウンターがクリアされる。その他カテゴリーには、AH (AH プロトコル処理部)、ALG (暗号化・認証アルゴリズム処理部)、COMP (IPComp プロトコル処理部)、ESP (ESP プロトコル処理部)、MAIN (IPsec メインプロトコル処理部)、SAD (SA データベース)、SETUP (SA の構築と削除)、SPD (セキュリティポリシーデータベース) がある。カテゴリーはカンマ区切りで複数指定可能。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

SHOW IPSEC COUNTERS (91 ページ)

RESET IPSEC POLICY COUNTER

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

RESET IPSEC POLICY=*policy* COUNTER

policy: IPsec ポリシー名（1～23 文字）

解説

指定した IPsec ポリシーの統計カウンターをクリアする。

パラメーター

POLICY IPsec ポリシー名

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

SHOW IPSEC POLICY（96 ページ）

RESET IPSEC SA COUNTER

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

RESET IPSEC SA=*sa-id* COUNTER

sa-id: SA 番号 (0 ~ 65535)

解説

指定した SA の統計カウンターをクリアする。

SA の一覧は SHOW IPSEC SA コマンドで確認できる。

パラメーター

SA SA 番号

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

SHOW IPSEC SA (104 ページ)

RESET ISAKMP COUNTER

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

RESET ISAKMP COUNTER [= {GENERAL|MAIN|QUICK|SAD|SPD|XDB|IPSEC|INFO|
AGGRESSIVE|NETWORK|TRANSACTION}]

解説

ISAKMP モジュールの統計カウンターをクリアする。

パラメーター

COUNTER クリアするカウンターのカテゴリーを指定する。省略時はすべてのカウンターがクリアされる。カテゴリーには、GENERAL (一般情報)、MAIN (Main モード交換)、QUICK (Quick モード交換)、SAD (ISAKMP SA データベース)、SPD (ISAKMP セキュリティポリシーデータベース)、XDB (ISAKMP 交換データベース)、IPSEC (ISAKMP と IPsec のインターフェースカウンター)、INFO (Informational 交換)、AGGRESSIVE (Aggressive モード交換)、NETWORK (ISAKMP メッセージの送受信)、TRANSACTION (Transaction 交換) がある。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

SHOW ISAKMP COUNTERS (116 ページ)

SET IPSEC BUNDLESPECIFICATION

カテゴリー：IPsec / SA バンドルスペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

SET IPSEC BUNDLESPECIFICATION=*bspec-id* [EXPIRYKBYTES=1..200000000]
[EXPIRYSECONDS=300..31449600]

bspec-id: SA バンドルスペック番号 (0~255)

解説

SA バンドルスペックの設定パラメーターを変更する。

パラメーター

BUNDLESPECIFICATION SA バンドルスペック番号

EXPIRYKBYTES バンドル内 SA の有効期限 (Kbyte)。通信データ量がここで指定した量に達すると、該当 SA バンドルは再ネゴシエートされる。KEYMANAGEMENT パラメーターに ISAKMP を指定したときだけ有効。デフォルトは無期限。

EXPIRYSECONDS バンドル内 SA の有効期限 (秒)。バンドル作成後ここで指定した時間が経過すると、該当 SA バンドルは再ネゴシエートされる。KEYMANAGEMENT パラメーターに ISAKMP を指定したときだけ有効。デフォルトは 28800 秒 (8 時間)。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE IPSEC BUNDLESPECIFICATION (37 ページ)

DESTROY IPSEC BUNDLESPECIFICATION (49 ページ)

SHOW IPSEC BUNDLESPECIFICATION (89 ページ)

SET IPSEC POLICY

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
SET IPSEC POLICY=policy [ACTION={DENY|IPSEC|PERMIT}]
[BUNDLESPECIFICATION=bspec-id] [PEERADDRESS={ipadd|ANY|DYNAMIC}]
[LADDRESS={ANY|ipadd[-ipadd]}] [LMASK=ipadd] [LNAME={ANY|system-name}]
[LPORT={ANY|port}] [RADDRESS={ANY|ipadd[-ipadd]}] [RMASK=ipadd]
[RNAME={ANY|system-name}] [RPORT={ANY|port}] [TRANSPORTPROTOCOL={ANY|ESP|
GRE|ICMP|OSPF|RSVP|TCP|UDP|protocol}] [DFBIT={SET|COPY|CLEAR}] [GROUP={0|
1|2}] [IPROUTETEMPLATE=template] [ISAKMPPOLICY=isakmp-policy]
[SRCINTERFACE=interface] [UDPHEARTBEAT={TRUE|FALSE}] [UDPPORT=port]
[UDPTUNNEL={TRUE|FALSE}] [USEPFKEY={TRUE|FALSE}] [POSITION=pos]
```

policy: IPsec ポリシー名 (1~23 文字)

bspec-id: SA バンドルスペック番号 (0~255)

ipadd: IP アドレスまたはネットマスク

system-name: システム名 (1~120 文字。空白を含む場合はダブルクォートで囲む)

port: TCP/UDP ポート番号 (0~65535)

protocol: IP プロトコル番号 (0~255)

template: ルートテンプレート名 (1~31 文字。大文字小文字を区別しない)

isakmp-policy: ISAKMP ポリシー名 (1~24 文字。空白を含む場合はダブルクォートで囲む)

interface: IP インターフェース名 (eth0、ppp0 など)

pos: ポリシールールの位置 (1~50)

解説

IPsec ポリシーの設定パラメーターを変更する。

パラメーター

POLICY IPsec ポリシー名

ACTION 本ポリシーの条件 (LADDRESS、LMASK、LNAME、LPORT、RADDRESS、RMASK、RNAME、RPORT、TRANSPORTPROTOCOL) に適合したパケットに対する処理を指定する。IPSEC (BUNDLESPECIFICATION パラメーターで指定した SA バンドルによって処理する)、PERMIT (IPsec を使わない通常のパケット処理を行う)、DENY (パケットを破棄する) から選択する。

BUNDLESPECIFICATION SA バンドル作成時に用いる SA バンドルスペックを指定する。SA バンドルは、IPsec で使用するセキュリティプロトコルやアルゴリズムの情報をひとまとめにしたもの。本パラメーターは、ACTION に IPSEC を指定した場合のみ有効 (かつ必須)。

PEERADDRESS 対向 IPsec 装置の IP アドレス。相手の IP アドレスが不定かつ動的に変化する場合は DYNAMIC を指定する。また、任意の固定 IP アドレスの相手と接続する場合は ANY を指定する。DYNAMIC と ANY は、KEYMANAGEMENT に ISAKMP を指定した場合のみ有効

LADDRESS パケット選択パラメーター（セクター）の 1 つ。ポリシーの適用対象となるパケットのローカル側 IP アドレスを指定する。LMASK と組み合わせてサブネットを指定したり、ハイフンでアドレスの範囲を指定することもできる。省略時は ANY（すべて）

LMASK セクターの 1 つ。LADDRESS に対するネットマスクを指定する。省略時は 255.255.255.255

LNAME セクターの 1 つ。ローカル側システム名を指定する。本パラメーターは自アドレスが不定のときに指定するもので、ISAKMP のフェーズ 2 ID として対向装置に送信される。省略時は ANY（すべて）

LPORT セクターの 1 つ。ローカル側ポート番号。省略時は ANY（すべて）

RADDRESS セクターの 1 つ。ポリシーの適用対象となるパケットのリモート側 IP アドレス。RMASK と組み合わせてサブネットを指定したり、ハイフンでアドレスの範囲を指定することもできる。省略時は ANY（すべて）

RMASK セクターの 1 つ。RADDRESS に対するネットマスク。省略時は 255.255.255.255

RNAME セクターの 1 つ。リモート側システム名を指定する。本パラメーターは対向装置のアドレスが不定のときに指定するもので、相手の ISAKMP のフェーズ 2 ID を指定する。省略時は ANY（すべて）

RPORT セクターの 1 つ。リモート側ポート番号。省略時は ANY（すべて）

TRANSPORTPROTOCOL セクターの 1 つ。ポリシーの適用対象となるパケットの IP プロトコルタイプ。ALL、TCP、UDP などの定義済み文字列か IP プロトコル番号で指定する。省略時は ANY（すべて）

DFBIT トンネルモード SA において、外側 IP ヘッダーの DF（Don't Fragment）ビットにどのような値を設定するかを指定する。COPY を指定した場合は、内側 IP ヘッダーの DF ビットの値をそのまま使用する。SET を指定した場合は、常にビットをオンにする。CLEAR を指定した場合は、常にビットをオフにする。インターネット上には異なる MTU を持つネットワークが混在しているため、DF ビットが立っているパケットはフラグメント不可により破棄される可能性があるため、通常は CLEAR を指定する。省略時は CLEAR

GROUP IKE フェーズ 2（Quick モード）での Diffie-Hellman 鍵交換に使用する Oakley グループ。PFS（Perfect Forward Secrecy）を有効にしている場合（USEPFSKEY パラメーターに TRUE を指定した場合）のみ有効。省略時はグループ 1

IPROUTETEMPLATE IP ルートテンプレート名。この IPsec ポリシーに基づいて IPsec SA が作成されたときに自動登録する経路エントリーのテンプレートを指定する。登録される経路の宛先アドレスは、IPsec SA のリモート側 IP アドレス/マスクとなる。本パラメーターは、ACTION が IPSEC で、PEERADDRESS が ANY か DYNAMIC のときのみ有効。省略時はなし

ISAKMPPOLICY ISAKMP ポリシー名。ACTION に IPSEC を指定した場合のみ有効。通常指定する必要はないが、同じ PEER を持つ ISAKMP ポリシーが複数存在するときに、この IPsec ポリシーで使用する ISAKMP ポリシーを明示的に指定したい場合に使う

SRCINTERFACE IPsec パケットの始点インターフェース。本パラメーターを指定した場合、IPsec パケットの始点アドレスにここで指定したインターフェースのアドレスが使用される。省略時は、パケットを送出するインターフェースのアドレスが使用される。送出インターフェースが Unnumbered の場合は、本パラメーターで始点アドレスを明示的に指定するとよい

UDPHEARTBEAT UDP ハートビートを使用するかどうか。UDP ハートビートは、UDP トンネリング（ESP over UDP）使用時にセッション情報が NAT 機器の変換テーブルから消えてしまうことを防ぐ本製品の独自機能。TRUE を指定した場合は、対向 IPsec ルーターの UDP ポート 2746 番宛てに 30

秒間隔でハートビートパケットを送信する。このパケットはセッション維持だけを目的としているため、受信しても特別な処理は行われない。省略時は FALSE

UDPPORT UDP トンネリング (ESP over UDP) パケットの送信先 UDP ポート。デフォルトは 2746 番

UDPTUNNEL UDP トンネリング (ESP over UDP) を使用するかどうか。TRUE を指定した場合は、IPsec (ESP) パケットを UDP でカプセル化して対向ルーターの 2746 番ポート (UDPPORT パラメーターで変更可能) 宛てに送信する。これにより、IPsec 装置間に NAT 機器があるような環境でも IPsec を使用できる。ただし、AH は使用できない。省略時は FALSE

USEPFSKEY PFS (Perfect Forward Secrecy) の有効・無効。PFS とは、ある鍵の解読が他の鍵の解読の手がかりにならないような性質を言う。PFS を有効にすると、IPsec SA 鍵の生成・更新時に Diffie-Hellman アルゴリズムを再実行するようになる。自動鍵管理 (KEYMANAGEMENT=ISAKMP) のときのみ有効。省略時は FALSE

POSITION IPsec ポリシーリスト内における本ポリシーの位置。省略時はリストの最後尾に追加される。ポリシーリストは、適用インターフェース (INTERFACE) ごとに個別管理される

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

ADD IP ROUTE TEMPLATE (「IP」の 187 ページ)

CREATE IPSEC POLICY (39 ページ)

DESTROY IPSEC POLICY (50 ページ)

DISABLE IPSEC POLICY DEBUG (54 ページ)

ENABLE IPSEC POLICY DEBUG (59 ページ)

SHOW IPSEC POLICY (96 ページ)

SET IPSEC SASPECIFICATION

カテゴリー：IPsec / SA スペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
SET IPSEC SASPECIFICATION=saspec-id [MODE={TRANSPORT|TUNNEL}]
    [COMPALGORITHM=LZS] [ENCALGORITHM={DES|3DESOUTER|NULL}] [ENCKEY=key-id]
    [HASHALGORITHM={MD5|NULL|SHA}] [HASHKEY=key-id] [INSPI=spi] [OUTSPI=spi]
    [ANTIREPLAYENABLED={TRUE|FALSE}] [REPLAYWINDOWSIZE={32|64|128|256}]
```

saspec-id: SA スペック番号 (0～255)

key-id: 鍵番号 (0～65535)

spi: SPI 値 (0～4294967295。ただし、0～255 は使用すべきでない)

解説

SA スペックの設定パラメーターを変更する。

パラメーター

SASPECIFICATION SA スペック番号

MODE SA の動作モード。TUNNEL (トンネルモード) と TRANSPORT (トランスポートモード) がある。省略時は TUNNEL

COMPALGORITHM 圧縮アルゴリズム。選択肢は LZS のみ

ENCALGORITHM 暗号化アルゴリズム

ENCKEY 暗号鍵番号。手動鍵管理で ESP を使う場合にのみ有効

HASHALGORITHM メッセージ認証用のハッシュアルゴリズム

HASHKEY 認証鍵番号。手動鍵管理で AH か ESP を使う場合にのみ有効

INSPI 内向きトラフィックの SPI (Security Parameter Index) 値。手動鍵管理で AH か ESP を使う場合にのみ有効

OUTSPI 外向きトラフィックの SPI (Security Parameter Index) 値。手動鍵管理で AH か ESP を使う場合にのみ有効

ANTIREPLAYENABLED リプレイ防止機能の有効・無効。PROTOCOL に COMP を指定した場合、および、手動鍵管理を使う場合は無効。デフォルトは FALSE

REPLAYWINDOWSIZE リプレイ防止ウィンドウサイズ。デフォルトは 32 パケット。自動鍵管理で AH か ESP を使う場合にのみ有効

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE IPSEC SASPECIFICATION (43 ページ)

DESTROY IPSEC SASPECIFICATION (51 ページ)

SHOW IPSEC SASPECIFICATION (111 ページ)

SET IPSEC UDPPORT

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

SET IPSEC UDPPORT=port

port: UDP ポート番号 (0 ~ 65535)

解説

UDP トンネリング (ESP over UDP) パケットを送受信する UDP ポートを変更する。デフォルトは 2746 番。

パラメーター

UDPPORT UDP ポート番号。デフォルトは 2746

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

SHOW IPSEC (88 ページ)

SET ISAKMP POLICY

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

```
SET ISAKMP POLICY=policy [AUTHTYPE={PRESHARED|RSASIG|RSAENCR}]
    [DHEXPONENTLENGTH=160..1023] [ENCALG={DES|3DESOUTER}]
    [EXPIRYKBYTES=1..1000] [EXPIRYSECONDS=600..31449600] [GROUP={0|1|2}]
    [HASHALG={SHA|MD5}] [HEARTBEATMODE={BOTH|NONE|RECEIVE|SEND}]
    [HYBRIDXAUTH={ON|OFF}] [KEY=0..65535] [LOCALID={ipadd|domain-name|
userdomainname|dist-name}] [LOCALRSAKEY=0..65535] [MODE={MAIN|
AGGRESSIVE}] [MSGRETRYLIMIT=0..1024] [MSGTIMEOUT=1..86400]
    [PHASE2XCHGLIMIT={NONE|1..1024}] [POLICYFILENAME=filename]
    [PRENEGOTIATE={TRUE|FALSE}] [REMOTEID={ipadd|domain-name|userdomainname|
dist-name}] [SENDDELETES={TRUE|FALSE}] [SENDNOTIFY={TRUE|FALSE}]
    [SENDIDALWAYS={TRUE|FALSE}] [SETCOMMITBIT={TRUE|FALSE}]
    [SRCINTERFACE=interface] [XAUTH={CLIENT|SERVER|NONE}]
    [XAUTHNAME=username] [XAUTHPASSWORD=password] [XAUTHTYPE={GENERIC|
RADIUS}]
```

policy: ISAKMP ポリシー名 (1~24 文字)

ipadd: IP アドレス

domain-name: ドメイン名

userdomainname: ユーザー名付きドメイン名 (user@foo.bar.xxx の形式)

dist-name: X.500 識別名 (DN) ("cn=myname,o=myorg,c=jp" の形式)

filename: ファイル名 (拡張子は.scp)

interface: IP インターフェース名 (eth0、ppp0 など)

username: ユーザー名 (1~64 文字)

password: パスワード (1~64 文字。大文字小文字を区別する)

解説

ISAKMP ポリシーの設定パラメーターを変更する。

パラメーター

POLICY ISAKMP ポリシー名

AUTHTYPE ISAKMP ピアの認証方式。PRESHARED (事前共有鍵)、RSASIG (RSA デジタル署名)、RSAENCR (RSA 公開鍵暗号) から選択する。デフォルトは PRESHARED。

DHEXPONENTLENGTH Diffie-Hellman 鍵交換アルゴリズムにおいて、各当事者が生成する乱数 ($g^a \bmod p$ における a) の長さ (ビット)。値が大きいほど生成した鍵の安全性が高まるが、鍵の交換に時間がかかるようになる。Oakley グループ 0、1、2 いずれの場合も最小値は 160 ビット。デフォルト値も同じく 160 ビット。最大値はグループによって異なり、グループ 0 は 511 ビット、グループ 1

は 767 ビット、グループ 2 は 1023 ビット。

ENCALG ISAKMP メッセージの暗号化アルゴリズム。デフォルトは DES。

EXPIRYKBYTES ISAKMP SA の有効期限 (Kbyte)。通信データ量が指定量に達すると、ISAKMP SA は再ネゴシエートされる。デフォルトは NONE (無期限)。

EXPIRYSECONDS ISAKMP SA の有効期限 (秒)。SA 作成後、指定時間が経過すると、ISAKMP SA は再ネゴシエートされる。デフォルトは 86400 (24 時間)。

GROUP 鍵交換時に用いる Diffie-Hellman (Oakley) グループを指定する。グループ 0 (512 ビット MODP)、グループ 1 (768 ビット MODP)、グループ 2 (1024 ビット MODP) から選択する。デフォルトはグループ 1。

HASHALG ISAKMP メッセージの認証用ハッシュアルゴリズム。デフォルトは SHA。

HEARTBEATMODE ISAKMP ハートビートを使用するかどうか。ISAKMP ハートビートは、ルーター間の通信が途絶えたときに古い SA 情報が残らないようにする本製品の独自機能。他社製品との互換性はない。SEND を指定した場合は、20 秒間隔でハートビートメッセージを送信する。RECEIVE を指定した場合は、ハートビートメッセージの受信だけを行う。受信側は、3 回連続してハートビートを受信できなかった場合は通信が不可能になったものとみなして、対向ルーターとの間に張られた SA をすべて削除する。BOTH を指定したときは送信と受信の両方を行う。NONE はハートビートメッセージを使用しないことを示す。デフォルトは NONE。

HYBRIDXAUTH ハイブリッド型の拡張認証 (XAUTH) を使用するかどうか。AUTHTYPE に RSASIG を指定した場合にのみ有効。デフォルトは OFF。

KEY ISAKMP ピアの認証に用いる鍵の番号を指定する。事前共有鍵 (PRESHARED) 方式の場合は各ピア共通の GENERAL 鍵 (必須) を、デジタル署名 (RSASIG) 方式の場合は ISAKMP ピアの RSA 公開鍵を指定する。無指定の場合は、ISAKMP メッセージで相手の公開鍵証明書を要求し、CA 証明書を使って鍵の正当性を検証する。公開鍵暗号 (RSAENCR) 方式の場合は、ISAKMP ピアの RSA 公開鍵を指定する。無指定の場合は、ISAKMP ピアの IP アドレス (PEER) を元に ENCO モジュールの鍵データベースが検索される。

LOCALID ISAKMP フェーズ 1 において、相手に送信する ID ペイロードの内容 (自分の ID 情報) を指定する。IP アドレス (例: 172.16.10.5)、ドメイン名 (例: bar.mydomain.net)、ユーザー名付きドメイン名 (例: joger@bar.mydomain.net)、X.500 識別名 (例: "cn=joge,o=ournet,c=jp") の 4 形式が使用できる。デフォルトでは、ISAKMP パケットの始点アドレスが ID として使われる。また、相手認証にデジタル署名 (RSASIG) 方式を使っている場合は、SET SYSTEM DISTINGUISHEDNAME コマンドで設定したシステム識別名 (DN) が使用される。このパラメーターは、おもに自分の IP アドレスが不定な場合に使う。

LOCALRSAKEY 自分の RSA 秘密鍵を指定する。相手認証にデジタル署名 (RSASIG) 方式か公開鍵暗号 (RSAENCR) 方式を使う場合の必須パラメーター。ただし、ENABLE ISAKMP コマンドの LOCALRSAKEY パラメーターでデフォルト鍵を設定している場合は省略可能。その場合、デフォルト鍵が使われる。

MODE ISAKMP フェーズ 1 で使用する IKE 交換モード。ID 情報が保護される MAIN モードと ID 情報が保護されない AGGRESSIVE モードがある。相手認証に事前共有鍵 (PRESHARED) 方式を使い、なおかつ、片側のルーターのアドレスが不定な場合は、LOCALID/REMOTEID で IP アドレス以外の ID を指定し、AGGRESSIVE モードを使う必要がある。それ以外の場合は通常 MAIN モードを使う。デフォルトは MAIN モード。

MSGRETRYLIMIT ISAKMP メッセージの再送回数。デフォルトは 5

MSGTIMEOUT ISAKMP メッセージを送信してから 1 回目の再送を行うまでの待ち時間。2 回目以降の再送待ち時間はこれよりも長くなる。デフォルトは 20 秒

PHASE2XCHGLIMIT このポリシーに基づいて確立された ISAKMP SA 上で行うことのできる IKE フェーズ 2 交換の最大数。デフォルトは NONE (制限なし)

POLICYFILENAME AT-VPN Client に送るセキュリティポリシーファイルの名前を指定する。本機能を使用するには、ENABLE ISAKMP コマンドの POLICYSERVERENABLED パラメーターに TRUE を設定する必要がある。詳細は AT-VPN Client のマニュアルを参照。

PRENEGOTIATE ルーター起動時 (正確には ENABLE ISAKMP コマンドの実行時) に IKE のネゴシエーションを行っておくかどうかを指定する。デフォルトは FALSE。

REMOTEID ISAKMP フェーズ 1 において、相手から受け取れることを期待する ID ペイロードの内容 (相手の ID 情報) を指定する。IP アドレス (例: 172.16.10.5) ドメイン名 (例: bar.mydomain.net) ユーザー名付きドメイン名 (例: joger@bar.mydomain.net) X.500 識別名 (例: "cn=joge,o=ournet,c=jp") の 4 形式が使用できる。デフォルトでは、相手から受け取った ISAKMP メッセージの始点 IP アドレスを ID 値として期待する。このパラメーターは、おもに相手ルーターの IP アドレスが不定な場合に使う。

SENDDELETES SA の削除を通知する Delete ペイロードを送信するかどうか。TRUE または ON を指定した場合、ローカル側で SA 情報が削除された場合に該当 SA がもはや有効でないことを相手ルーターに通知する。これにより、無効な SA にトラフィックが送り出されることを防止できる。デフォルトは FALSE。

SENDNOTIFY IKE のステータスやエラー情報を通知する Notify ペイロードを送信するかどうか。デフォルトは FALSE。

SENDIDALWAYS ISAKMP SA のネゴシエーション時に常に ID ペイロードを送信するかどうか。デフォルトは FALSE。

SETCOMMITBIT ISAKMP SA のネゴシエーション時に ISAKMP ヘッダーの Commit ビットをオンにするかどうか。TRUE または ON を指定した場合は、SA 確立の確認メッセージを受け取るまで、SA にトラフィックが送信されないことが保証される。デフォルトは FALSE。

SRCINTERFACE ISAKMP メッセージの始点インターフェース。指定したインターフェースに有効な IP アドレスが設定されている場合は、そのアドレスが ISAKMP メッセージの始点アドレスとして使われる。

XAUTH ISAKMP フェーズ 1 終了後に拡張認証 (XAUTH) を使用するかどうか。使用する場合はサーバー (認証する側) クライアント (認証を受ける側) のどちらになるかを指定する。SERVER 指定時は、ISAKMP ピアに対して XAUTH の認証要求を送る。CLIENT 指定時は、ISAKMP ピアからの XAUTH 認証要求を期待する。NONE は XAUTH を使わない。デフォルトは NONE。

XAUTHNAME XAUTH 使用時のユーザー名。クライアント側が指定する。

XAUTHPASSWORD XAUTH 使用時のパスワード。クライアント側が指定する。

XAUTHTYPE XAUTH 使用時の認証方式。GENERAL (ユーザー認証データベース) または RADIUS から選択する。デフォルトは GENERIC。

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE ISAKMP POLICY (45 ページ)

DESTROY ISAKMP POLICY (52 ページ)

SHOW ISAKMP POLICY (122 ページ)

SHOW IPSEC

カテゴリー：IPsec / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW IPSEC

解説

IPsec モジュールの状態を表示する。

入力・出力・画面例

```
SecOff > show ipsec

IPSEC Module Configuration

Module Status ..... ENABLED
IPsec over UDP
  Status ..... CLOSED
  Listen Port ..... 2746
```

Module Status	IPsec モジュールの有効・無効
IPsec over UDP/Status	UDP トンネリング (ESP over UDP) の有効・無効
IPsec over UDP/Listen Port	UDP トンネリングパケットの送受信ポート番号

表 6:

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

DISABLE IPSEC (53 ページ)
ENABLE IPSEC (58 ページ)

SHOW IPSEC BUNDLESPECIFICATION

カテゴリー：IPsec / SA バンドルスペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW IPSEC BUNDLESPECIFICATION [=bspec-id]

bspec-id: SA バンドルスペック番号 (0~255)

解説

SA バンドルスペックに関する情報を表示する。

パラメーター

BUNDLESPECIFICATION SA バンドルスペック番号。省略時はすべての SA バンドルスペックの情報が簡潔に表示される。指定時は、該当バンドルスペックの詳細情報が表示される。

入力・出力・画面例

```
SecOff > show ipsec bundlespecification

ID  KeyManagement  ExpKBytes  ExpSec  String
-----
 1  ISAKMP                -   28800  1

SecOff > show ipsec bundlespecification=1

Bundle Specification

Id ..... 1
Key Management ..... ISAKMP
String ..... 1
Expiry Kilobytes ..... -
Expiry Seconds ..... 28800

Num of Proposals..... 1

Proposal ..... 1
  ProposalNumber ..... 1
  Protocol ..... ESP
  Number Of Transforms ..... 1
    Transform 0 ..... SA Spec Id    1
```

ID	SA バンドルスペック番号
KeyManagement	鍵管理方式。MANUAL（手動）か ISAKMP（自動）
ExpKBytes	SA の有効期限（KByte）。通信量がこの値を超えると SA の再ネゴシエートが行われる
ExpSec	SA の有効期限（秒）。SA 作成後この時間が経過すると SA の再ネゴシエートが行われる
String	バンドルを構成する SA スペックのリスト

表 7: SA バンドルスペック番号未指定時

Id	SA バンドルスペック番号
Key Management	鍵管理方式。MANUAL（手動）か ISAKMP（自動）
String	バンドルを構成する SA スペックのリスト
ExpiryKBytes	SA の有効期限（KByte）。通信量がこの値を超えると SA の再ネゴシエートが行われる
ExpirySeconds	SA の有効期限（秒）。SA 作成後この時間が経過すると SA の再ネゴシエートが行われる
Num of Proposals	バンドルスペック内のプロポーザル数
Proposal	プロポーザル数
Proposal Number	プロポーザル番号
Protocol	IPsec プロトコル。ESP、AH、COMP のいずれか
Number of Transforms	トランスフォーム数
Transform	トランスフォーム番号と関連する SA スペック番号

表 8: SA バンドルスペック番号指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

CREATE IPSEC BUNDLESPECIFICATION（37 ページ）
DESTROY IPSEC BUNDLESPECIFICATION（49 ページ）
SET IPSEC BUNDLESPECIFICATION（77 ページ）

SHOW IPSEC COUNTERS

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW IPSEC COUNTERS [= {AH|ALG|COMP|ESP|MAIN|SAD|SETUP|SPD}]

解説

IPsec モジュールのデバッグ用統計カウンターを表示する。

パラメーター

COUNTERS 表示する統計カウンターのカテゴリーを指定する。省略時および ALL を指定した場合はすべてのカウンターが表示される。その他カテゴリーには、AH (AH プロトコル処理部)、ALG (暗号化・認証アルゴリズム処理部)、COMP (IPComp プロトコル処理部)、ESP (ESP プロトコル処理部)、MAIN (IPsec メインプロトコル処理部)、SAD (SA データベース)、SETUP (SA の構築と削除)、SPD (セキュリティポリシーデータベース) がある。カテゴリーはカンマ区切りで複数指定可能。

入力・出力・画面例

```
SecOff > show ipsec counters
```

SAD Counters

	Good	Failed
Find SA	3407	0
Get SA	18110	0
Add SA	8	
Delete SA	7	0

SPD Counters

	Good	Failed
policyMatchSelectors	11361	18812
policyAdd	3	0
policyGet	20	3
policyDelete	0	0
policyGetConfig	2	0
policySetConfig	1	0
policyFindByPeer	0	0
saSpecAdd	1	0
saSpecGet	17	1
saSpecDelete	0	0
bundleSpecAdd	1	0
bundleSpecGet	10	1

SHOW IPSEC COUNTERS

bundleSpecDelete	0	0	
Policy Filter Counters			
localAddressMaskFailed	7523	localAddressRangeFailed	0
remoteAddressMaskFailed	0	remoteAddressRangeFailed	0
localPortFailed	11289	remotePortFailed	0
localNameFailed	0	remoteNameFailed	0
transportProtoFailed	0		
IPsec bundle setup/remove counters:			
setupGetSaSpecFail	0	setupGetPolicyFail	0
setupStarted	8	setupSaSetupFailImm	0
setupSaSetupStarted	8	setupSaSetupFailed	0
setupDone	8	setupFailed	0
setupBundleRemoving	0		
removeStarted	7	removeSaSetupStarted	0
removeDone	7		
IPsec main packet processing counters:			
outProcessPkt	8001	inProcessPkt	6767
outNoPolicyFound	0	inNoPolicyFound	0
outProcessPktFinished	3766	inProcessPktFinished	3391
IPsec over UDP Counters			
outPkt	0	inPkt	0
outPktFail	0	inPktBadVersion	0
		inPktNoPolicy	0
outUdpHeartBeat	0	inUdpHeartBeat	0
ESP setup/remove counters			
setupGetSaFailed	0	setupEncSetupFailed	0
setupHashSetupFailImm	0	setupEncSetupBundleRm	0
setupFailed	0	setupDone	8
removeGetSaFailed	0	removeNothingDone	0
removeHashFailImm	0	removeDone	7
ESP outbound processing counters			
bufChainCopy	0	seqNumberCycled	0
encryptionStart	3766	encryptionFailImm	0
encDoneGetSaFail	0	encryptionFail	0
encDoneSaBadState	0	encryptionGood	3766
hashStart	3766	hashFailImm	0
hashDoneGetSaFail	0	hashFail	0
hashDoneSaBadState	0	hashGood	3766
ESP inbound processing counters			
bufChainCopy	0	icvInvalid	0
paddingInvalid	0	replayedPacket	0
hashStart	3391	hashFailImm	0
hashDoneGetSaFail	0	hashFail	0
hashDoneSaBadState	0	hashGood	3391
decryptionStart	3391	decryptionFailImm	0
encDoneGetSaFail	0	decryptionFail	0

```

encDoneSaBadState          0  decryptionGood          3391

AH setup/remove counters
  setupGetSaFailed          0  setupFailed              0
  setupDone                  0
  removeGetSaFailed          0  removeNothingDone        0
  removeDone                  0
AH outbound processing counters
  bufChainCopy               0
  seqNumberCycled            0  fragmentSeen              0
  hashStart                   0  hashFailImm               0
  hashDoneGetSaFail          0  hashFail                   0
  hashDoneSaBadState         0  hashGood                   0
AH inbound processing counters
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
bufChainCopy                0  replayedPacket            0
  icvInvalid                  0  badPayloadLength          0
  hashStart                     0  hashFailImm                0
  hashDoneGetSaFail            0  hashFail                    0
  hashDoneSaBadState           0  hashGood                    0

COMP setup/remove counters:
  setupGetSaFailed            0  setupFailed                0
  setupDone                    0
  removeGetSaFailed            0  removeNothingDone          0
  removeDone                    0
COMP outbound processing counters:
  bufChainCopy                0
  compTooSmall                 0  compFragment                0
  nonExpansionBackoff           0  dataExpansion                0
  compressionStart              0  compressionFailImm          0
  compDoneGetSaFail             0  compressionFail              0
  compDoneSaBadState            0  compressionGood              0
COMP inbound processing counters:
  bufChainCopy                0
  decompressionStart            0  decompressionFailImm         0
  decompDoneGetSaFail           0  decompressionFail            0
dec
ompDoneSaBadState            0  decompressionGood            0

General Algorithm Counters
  nullKeymatProcessed          0
  DES:
    desKeymatProcessed          8
    desAttachFail              0  desAttachGood                8
    desConfigureFail            0  desConfigureGood              8
    desRemove                    7  desDetached                    7
    desEncodeGood              7532  desDecodeGood                  6782
    desEncodeFail                0  desDecodeFail                  0
    desEncodeDiscard             0  desDecodeDiscard              0
    desEncodeGetInfoFail         0

```

SHOW IPSEC COUNTERS

TRIPLE DES INNER:			
3DesInnerKeymatProcessed	0		
3DesInnerAttachFail	0	3DesInnerAttachGood	0
3DesInnerConfigureFail	0	3DesInnerConfigureGood	0
3DesInnerRemove	0	3DesInnerDetached	0
3DesInnerEncodeGood	0	3DesInnerDecodeGood	0
3DesInnerEncodeFail	0	3DesInnerDecodeFail	0
3DesInnerEncodeDiscard	0	3DesInnerDecodeDiscard	0
3DesInnerEncGetInfoFail	0		
TRIPLE DES OUTER:			
3DesOuterKeymatProcessed	0		
3DesOuterAttachFail	0	3DesOuterAttachGood	0
3DesOuterConfigureFail	0	3DesOuterConfigureGood	0
3DesOuterRemove	0	3DesOuterDetached	0
3DesOuterEncodeGood	0	3DesOuterDecodeGood	0
3DesOuterEncodeFail	0	3DesOuterDecodeFail	0
3DesOuterEncodeDiscard	0	3DesOuterDecodeDiscard	0
3DesOuterEncGetInfoFail	0		
TRIPLE DES 2KEY:			
3Des2KeyKeymatProcessed	0		
3Des2KeyAttachFail	0	3Des2KeyAttachGood	0
3Des2KeyConfigureFail	0	3Des2KeyConfigureGood	0
3Des2KeyRemove	0	3Des2KeyDetached	0
3Des2KeyEncodeGood	0	3Des2KeyDecodeGood	0
3Des2KeyEncodeFail	0	3Des2KeyDecodeFail	0
3Des2KeyEncodeDiscard	0	3Des2KeyDecodeDiscard	0
3Des2KeyEncGetInfoFail	0		
SHA:			
shaKeymatProcessed	8		
shaAttachFail	0	shaAttachGood	8
shaConfigureFail	0	shaConfigureGood	8
shaRemove	7	shaDetached	7
shaEncodeGood	7532	shaDecodeGood	6782
shaEncodeFail	0	shaDecodeFail	0
shaEncodeDiscard	0	shaDecodeDiscard	0
MD5:			
md5KeymatProcessed	0		
md5AttachFail	0	md5AttachGood	0
md5ConfigureFail	0	md5ConfigureGood	0
md5Remove	0	md5Detached	0
md5EncodeGood	0	md5DecodeGood	0
md5EncodeFail	0	md5DecodeFail	0
md5EncodeDiscard	0	md5DecodeDiscard	0
DES-MAC:			
desmacKeymatProcessed	0		
desmacAttachFail	0	desmacAttachGood	0
desmacConfigureFail	0	desmacConfigureGood	0
desmacRemove	0	desmacDetached	0
desmacEncodeGood	0	desmacDecodeGood	0
desmacEncodeFail	0	desmacDecodeFail	0
desmacEncodeDiscard	0	desmacDecodeDiscard	0

LZS:			
lzsKeymatProcessed	0		
lzsAttachFail	0	lzsAttachGood	0
lzsConfigureFail	0	lzsConfigureGood	0
lzsRemove	0	lzsDetached	0
lzsEncodeGood	0	lzsDecodeGood	0
lzsEncodeFail	0	lzsDecodeFail	0
lzsEncodeDiscard	0	lzsDecodeDiscard	0

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

SHOW IPSEC SA（104 ページ）

SHOW IPSEC POLICY

カテゴリー：IPsec / IPsec ポリシー

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW IPSEC POLICY[=*policy*] [*SABUNDLE*] [*COUNTERS*]

policy: IPsec ポリシー名（1～23 文字）

解説

IPsec ポリシーに関する情報を表示する。

パラメーター

POLICY IPsec ポリシー名。省略時はすべての IPsec ポリシーの情報を簡潔に表示する。指定時は、該当ポリシーの詳細情報を表示する。

SABUNDLE 該当 IPsec ポリシーに基づいて作成された SA バンドルの情報だけを表示する。

COUNTERS 該当 IPsec ポリシーの統計カウンターを表示する。

入力・出力・画面例

```
SecOff > show ipsec policy
```

Interface	Name	Action	KeyManagement	Position
ppp0	isa	PERMIT	-	1
ppp0	vpn	IPSEC	ISAKMP	2
ppp0	inet	PERMIT	-	3

```
SecOff > show ipsec policy=vpn
```

Ipsec Policy Information

```
Name ..... vpn
Interface ..... ppp0
Position ..... 2
Action ..... IPSEC
Key Management ..... ISAKMP
Isakmp Policy Name .....
Bundle Specification ..... 1
Peer IP Address Dynamic ..... FALSE
Peer IP Address Any ..... FALSE
Local IP Address Dynamic ..... TRUE
Lower Layer Available ..... TRUE
Activating Lower Layer ..... FALSE
```



```

Peer IP Address ..... 1.1.1.1
Local IP Address ..... 63.12.66.74
Use PFS Key ..... FALSE
Group..... 1
Filter:
  Local Address ..... 192.168.20.0
  Local Mask ..... 255.255.255.0
  Local Port ..... ANY
  Local Name ..... ANY
  Remote Address ..... 192.168.1.0
  Remote Mask ..... 255.255.255.0
  Remote Port ..... ANY
  Remote Name ..... ANY
  Transport Protocol ..... ANY
  Sa Selector From Pkt ..... 00000000
DF Bit ..... CLEAR
UDP Tunnel ..... FALSE
  Peer Port ..... -
  Peer IP Address ..... -
  Internal IP Address ..... -
  HeartBeats Enabled ..... -
Debug device ..... 16
Filter debug flags ..... 00000000
Packet debug flags ..... 00000000
Trace debug flags ..... 00000000
Packet debug length ..... 72
Max Out Packet queue length .... 20
Number of Out Packets queued ... 0

```

Bundles

Bundle		Expiry Limits - hard/soft/used		
Index	SA's	State	Bytes	Seconds
0	1	VALID	-/-/34910	28800/27360/109

SecOff > show ipsec policy sabundle

Ipssec Policy SA Bundles

Bundle		Expiry Limits - hard/soft/used		
Index	SA's	State	Bytes	Seconds
Policyvpn				
0	1	VALID	-/-/302062	28800/27360/446

SecOff > show ipsec policy=vpn counters

Setup/Remove Counters:

setupStarted	2	setupSaSetupFailImm	0
setupSaSetupStarted	2	setupSaSetupFailed	0

SHOW IPSEC POLICY

setupDone	2	setupFailed	0
removeStarted	1	removeSaSetupStarted	0
removeDone	1		
Outbound Packet Processing Counters:			
outDeny	0	outPermit	0
outNoBundle	12	outNoBundleFail	0
outMakeSetupStrctFail	0	outSetupBundleFail	0
outBundleSoftExpire	0	outBundleExpire	0
outProcessStart	514	outProcessFailImm	0
outBundleStateBad	0	outProcessFail	0
outProcessDone	514		
Inbound Packet Processing Counters:			
inDeny	0	inPermit	0
inCompUncompressed	0	inActionIpssecFail	0
inBundleStateBad	0	inNotFirstSaInBundle	0
inProcessStart	522	inProcessFailImm	0
inProcessFail	0	inProcessDone	522
inEndOfBundle	0	inPrematureEndBundle	0
inBundleSaMatchFail	0	inPolicyActionFail	0
inPolSelectMatchFail	0	inBundleReplaced	0
inBundleSoftExpire	0	inBundleExpire	0

Interface	対象インターフェース名
Name	IPsec ポリシー名
Action	アクション。IPSEC (IPsec 適用) PERMIT (通過) DENY (破棄) のいずれか
KeyManagement	鍵管理方式。MANUAL (手動) か ISAKMP (自動)
Position	ポリシー番号 (位置)

表 9: IPsec ポリシー名未指定時

Name	IPsec ポリシー名
Interface	対象インターフェース名
Position	ポリシー番号（位置）
Action	アクション。IPSEC（IPsec 適用）、PERMIT（通過）、DENY（破棄）のいずれか
Key Management	鍵管理方式。MANUAL（手動）か ISAKMP（自動）
Isakmp Policy Name	IKE フェーズ 1 のネゴシエーション時に使用する ISAKMP ポリシー名
Bundle Specification	使用する SA バンドルスペック番号
Peer IP Address Dynamic	PEER パラメーターに DYNAMIC（IP アドレスが動的に変化する相手だけを受け入れる）を指定したかどうか
Peer IP Address Any	PEER パラメーターに ANY（任意の固定 IP アドレスから IPsec SA のネゴシエーション要求を受け入れる）を指定したかどうか

Local IP Address Dynamic	ローカル側 IP アドレスが動的に決定されるかどうか
Peer IP Address	対向 IPsec 装置の IP アドレス (IPsec トンネルのリモート側終端アドレス)
IP Route Template	IP ルートテンプレート名
Local IP Address	ローカル側 IP アドレス (IPsec トンネルのローカル側終端アドレス)
Use PFS Key	Perfect Forward Security (PFS) を使用するかどうか
Group	Diffie-Hellman (Oakley) グループ
Filter	IPsec ポリシー適用対象のパケットを識別するフィルター (セレクター) の情報が表示される
Local Address	ローカル側 IP アドレス
Local Mask	ローカル側 IP アドレスに対するマスク
Local Port	ローカル側ポート
Local Name	ローカル側システム名
Remote Address	リモート側 IP アドレス
Remote Mask	リモート側 IP アドレスに対するマスク
Remote Port	リモート側ポート
Remote Name	リモート側システム名
Transport Protocol	トランスポート層プロトコル
SA Selector From Pkt	パケット内のどのフィールドを検索に使用するかを示すビットフラグ
DF Bit	外側 IP ヘッダーに付けるフラグメント不可フラグ (DF Bit) の値。COPY (内側のオリジナル IP ヘッダーからコピー)、SET (常にオン)、CLEAR (常にオフ)
Debug device	デバッグ情報の出力先デバイス (ポート) 番号
Filter debug flags	フィルターデバッグがオンに設定されているセレクターと許可/拒否の結果を示すフラグ
Packet debug flags	パケットデバッグがオンに設定されている処理部とパケットの向きを示すフラグ。パケットの一部も表示される
Trace debug flags	トレースデバッグのオン・オフを示すフラグ
Packet debug length	パケットデバッグ時に表示されるデータ長さ
Max Out Packet queue length	出力パケットキューの最大長
Number of Out Packets queued	現在出力キューに入っているパケットの数
Bundles	本ポリシーに基づいて作成された SA バンドルに関する情報が表示される
Index	SA バンドル ID
SAs	バンドル内の SA ID
State	SA バンドルの状態。VALID、INVALID、CREATING、REMOVING のいずれか

Expiry Limits - hard/soft/used	バンドル内 SA の有効期限。各 SA は、soft limit を超えると再ネゴシエートされ、hard limit を超えると SPD から削除される
ExpiryBytes	バンドル内 SA の有効期限（バイト数）。値は左から順に、削除期限（hard limit）、再ネゴシエーション期限（soft limit）、現在までの処理済みバイト数
ExpirySeconds	バンドル内 SA の有効期限（秒）。値は左から順に、削除期限（hard limit）、再ネゴシエーション期限（soft limit）、現在までの経過秒数

表 10: IPsec ポリシー名指定時

Policy	IPsec ポリシー名
Index	ポリシー別の SA バンドル ID
SAs	バンドル内の SA ID
State	SA バンドルの状態。VALID、INVALID、CREATING、REMOVING のいずれか
Expiry Limits - hard/soft/used	バンドル内 SA の有効期限。各 SA は、soft limit を超えると再ネゴシエートされ、hard limit を超えると SPD から削除される
ExpiryBytes	バンドル内 SA の有効期限（バイト数）。値は左から順に、削除期限（hard limit）、再ネゴシエーション期限（soft limit）、現在までの処理済みバイト数
ExpirySeconds	バンドル内 SA の有効期限（秒）。値は左から順に、削除期限（hard limit）、再ネゴシエーション期限（soft limit）、現在までの経過秒数

表 11: SABUNDLE オプション指定時

Setup/Remove Counters	SA バンドルの作成と削除に関するカウンターが表示される。setupStarted
setupSaSetupStarted	SA のセットアップ開始回数
setupDone	SA バンドルのセットアップ成功回数
removeStarted	SA バンドルの削除開始回数
removeDone	SA バンドルの削除成功回数
setupSaSetupFailImm	SA のセットアップ即時失敗回数
setupSaSetupFailed	SA セットアップ失敗回数
setupFailed	SA バンドルのセットアップ失敗回数
removeSaSetupStarted	SA の削除開始回数
Outbound Packet Processing Counters	外向き SA バンドルの処理に関するカウンターが表示される
outDeny	外向きパケットが DENY アクションの IPsec ポリシーにマッチした回数

outNoBundle	外向きパケットが SA バンドルを持たない IPsec ポリシーにマッチした回数
outMakeSetupStrctFail	セットアップ構造体の問題により、外向きパケット用 SA バンドルのセットアップに失敗した回数
outBundleSoftExpire	外向きパケットにより SA バンドルの再ネゴシエーション期限（バイト数）に到達した回数
outProcessStart	外向きパケットに対して IPsec 処理を開始した回数
outBundleStateBad	外向きパケットが有効なバンドルを持たない IPsec ポリシーにマッチした回数
outProcessDone	外向きパケットに対する IPsec 処理が完了した回数
outPermit	外向きパケットが PERMIT アクションの IPsec ポリシーにマッチした回数
outNoBundleFail	バンドルを持たない IPsec ポリシーにマッチしたため破棄された外向きパケットの数
outSetupBundleFail	外向きパケット用 SA バンドルのセットアップ失敗回数
outBundleExpire	外向きパケットにより SA バンドルの有効期限（バイト数）に到達した回数
outProcessFailImm	外向きパケットに対する IPsec 処理が即時失敗した回数
outProcessFail	外向きパケットに対する IPsec 処理に失敗した回数
Inbound Packet Processing Counters	内向き SA バンドルの処理に関するカウンターが表示される
inDeny	内向きパケットが DENY アクションの IPsec ポリシーにマッチした回数
inCompUncompressed	IPComp SA 上で圧縮されていないパケットを受信した回数
inBundleStateBad	有効なバンドルを持たない IPsec ポリシーにマッチした内向きパケットの数
inProcessStart	内向きパケットに対して IPsec 処理を開始した回数
inProcessFail	内向きパケットに対する IPsec 処理に失敗した回数
inEndOfBundle	内向きパケットに対し、SA バンドルによる処理が最後まで行われなかった回数
inBundleSaMatchFail	内向きパケットがバンドル内の SA にマッチしなかった回数
inPolSelectMatchFail	内向きパケットが IPsec ポリシーのセレクトターにマッチしなかった回数
inBundleSoftExpire	内向きパケットにより SA バンドルの再ネゴシエーション期限（バイト数）に到達した回数
inPermit	内向きパケットが PERMIT アクションの IPsec ポリシーにマッチした回数

inActionIpsecFail	内向きの平文パケットが IPSEC アクションの IPsec ポリシーにマッチした回数
inNotFirstSaInBundle	内向きパケットがバンドルの先頭でない SA にマッチした回数
inProcessFailImm	内向きパケットに対する IPsec 処理が即時失敗した回数
inProcessDone	内向きパケットに対する IPsec 処理が完了した回数
inPrematureEndBundle	バンドル内のすべての SA が使用される前に、内向きパケットに対する処理が完了した回数
inPolicyActionFail	内向き IPsec パケットがポリシーにマッチしなかった回数
inBundleReplaced	内向きパケットにより、古い SA バンドルが削除された回数
inBundleExpire	内向きパケットにより SA バンドルの有効期限（バイト数）に到達した回数

表 12: COUNTER オプション指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

CREATE IPSEC POLICY（39 ページ）

DESTROY IPSEC POLICY（50 ページ）

SET IPSEC POLICY（78 ページ）

SHOW IPSEC SA

カテゴリー：IPsec / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW IPSEC SA [=sa-id] [COUNTERS]

sa-id: SA 番号 (0~65535)

解説

SA データベース (SAD) 内の SA に関する情報を表示する。

パラメーター

SA SA 番号。省略時はすべての SA に関する情報を簡潔に表示する。指定時は該当する SA の詳細情報を表示する。

COUNTERS SA の統計カウンターを表示する。

入力・出力・画面例

```
SecOff > show ipsec sa
```

SA Id	Policy	Bundle	State	Protocol	OutSPI	InSPI
0	12	1	Valid	IPCOMP	3	3
1	12	1	Valid	ESP	1194036652	3877490456

```
SecOff > show ipsec sa=1
```

```
SA Id ..... 1
Policy ..... 12
Bundle ..... 1
SA Specification Used ..... 2
State ..... Valid
Protocol ..... ESP
Mode ..... TUNNEL
Outbound SPI ..... 1194036652
Inbound SPI ..... 3877490456
Local tunnel IP address ..... 63.12.123.233
Remote tunnel IP address ..... 1.1.1.1
Encryption algorithm ..... DES
Encryption ENCO channel..... 2
Hash algorithm ..... MD5
Hash ENCO channel..... 3
Filters
```



```

Remote IP address ..... 1.1.1.1
Remote IP address mask ..... 255.255.255.255
Local port number ..... 1701
Remote port number ..... 1701
Transport protocol ..... UDP
Local Name ..... ANY
Remote Name ..... ANY
DF Bit ..... CLEAR
Last sent sequence number ..... 331
Anti-replay checking enabled ..... FALSE
Debug device ..... 16
Filter debug flags ..... 00000000
Packet debug flags ..... 00000000
Trace debug flags ..... 00000000
Packet debug length ..... 72

SecOff > show ipsec sa counters

SA: 0
Outbound packet processing counters:
  outProcessStart          373  outProcessFailImm          0
  outProcessFail           0  outProcessDone             373
ESP:
  espOutBufChainCopy       0
  espEncryptionStart       0  espEncryptionFailImm       0
  espEncryptionFail        0  espEncryptionGood          0
  espOutHashStart          0  espOutHashFailImm          0
  espOutHashFail           0  espOutHashGood             0
AH:
  ahOutBufChainCopy        0
  ahSeqNumberCycled        0  ahFragmentSeen             0
  ahOutHashStart           0  ahOutHashFailImm           0
  ahOutHashFail            0  ahOutHashGood              0
IPCOMP:
  compOutBufChainCopy      340
  compTooSmall             0  compFragment                0
  nonExpansionBackoff      20  dataExpansion               341
  compressionStart        353  compressionFailImm         0
  compressionFail          0  compressionGood            353

Inbound packet processing counters:
  inProcessStart           8  inProcessFailImm           0
  inProcessFail            0  inProcessDone              8
ESP:
  espInBufChainCopy        0  espReplayedPacket          0
  espInHashStart           0  espInHashFailImm           0
  espInHashFail            0  espInHashGood              0
  espDecryptionStart       0  espDecryptionFailImm       0
  espDecryptionFail        0  espDecryptionGood          0
  espIcvInvalid            0  espPaddingInvalid          0
AH:

```

SHOW IPSEC SA

ahInBufChainCopy	0	ahReplayedPacket	0
ahBadPayloadLength	0	ahIcvInvalid	0
ahInHashStart	0	ahInHashFailImm	0
ahInHashFail	0	ahInHashGood	0
IPCOMP:			
compInBufChainCopy	0		
decompressionStart	8	decompressionFailImm	0
decompressionFail	0	decompressionGood	8
SA: 1			
Outbound packet processing counters:			
outProcessStart	373	outProcessFailImm	0
outProcessFail	0	outProcessDone	373
ESP:			
espOutBufChainCopy	18		
espEncryptionStart	373	espEncryptionFailImm	0
espEncryptionFail	0	espEncryptionGood	373
espOutHashStart	373	espOutHashFailImm	0
espOutHashFail	0	espOutHashGood	373
AH:			
ahOutBufChainCopy	0		
ahSeqNumberCycled	0	ahFragmentSeen	0
ahOutHashStart	0	ahOutHashFailImm	0
ahOutHashFail	0	ahOutHashGood	0
IPCOMP:			
compOutBufChainCopy	0		
compTooSmall	0	compFragment	0
nonExpansionBackoff	0	dataExpansion	0
compressionStart	0	compressionFailImm	0
compressionFail	0	compressionGood	0
Inbound packet processing counters:			
inProcessStart	363	inProcessFailImm	0
inProcessFail	0	inProcessDone	363
ESP:			
espInBufChainCopy	0	espReplayedPacket	0
espInHashStart	363	espInHashFailImm	0
espInHashFail	0	espInHashGood	363
espDecryptionStart	363	espDecryptionFailImm	0
espDecryptionFail	0	espDecryptionGood	363
espIcvInvalid	0	espPaddingInvalid	0
AH:			
ahInBufChainCopy	0	ahReplayedPacket	0
ahBadPayloadLength	0	ahIcvInvalid	0
ahInHashStart	0	ahInHashFailImm	0
ahInHashFail	0	ahInHashGood	0
IPCOMP:			
compInBufChainCopy	0		
decompressionStart	0	decompressionFailImm	0
decompressionFail	0	decompressionGood	0

SA Id	SA ID
Policy	該当 SA のもとになった IPsec ポリシー名
Bundle	SA が所属する SA バンドル ID
State	SA の状態。UNDEF、VALID、CREATING、REMOVING のいずれか
Protocol	SA が使用する IPsec プロトコル。ESP、AH、IPCOMP のいずれか
OutSPI	外向きトラフィックの SPI (Security Parameter Index)
InSPI	内向きトラフィックの SPI (Security Parameter Index)

表 13: SA 無指定時

SA Id	SA ID
Policy	該当 SA のもとになった IPsec ポリシー名
Bundle	SA が所属する SA バンドル ID
SA Specification Used	SA の作成に使用した SA スペック番号
State	SA の状態。UNDEF、VALID、CREATING、REMOVING のいずれか
Protocol	SA が使用する IPsec プロトコル。ESP、AH、IPCOMP のいずれか
CPI	IPComp SA の CPI (Compression Parameter Index)。IPComp SA でのみ表示
Mode	SA 動作モード。TUNNEL か TRANSPORT
Outbound SPI	外向きトラフィックの SPI (Security Parameter Index)
Inbound SPI	内向きトラフィックの SPI (Security Parameter Index)
Local tunnel IP address	IPsec トンネルのローカル側終端 IP アドレス。トンネルモードの場合のみ表示
Remote tunnel IP address	IPsec トンネルのリモート側終端 IP アドレス。トンネルモードの場合のみ表示
Encryption algorithm	ESP SA が使用する暗号アルゴリズム。ESP SA でのみ表示
Encryption ENCO channel	暗号化プロセスが使用する ENCO チャンネル番号。ESP SA でのみ表示
Hash algorithm	AH SA、ESP SA が使用する認証用ハッシュアルゴリズム。AH SA と ESP SA でのみ表示
Hash ENCO channel	ハッシュプロセスが使用する ENCO チャンネル番号。AH SA と ESP SA でのみ表示
Compression algorithm	IPComp SA が使用する圧縮アルゴリズム。IPComp SA でのみ表示
Compression ENCO channel	圧縮プロセスが使用する ENCO チャンネル番号。IPComp SA でのみ表示
Filters	SA の元になった IPsec ポリシーのパケットセクターに関する情報が表示される

Local IP address	ローカル側 IP アドレス
Local IP address mask	ローカル側 IP アドレスに対するマスク
Remote IP address	リモート側 IP アドレス
Remote IP address mask	リモート側 IP アドレスに対するマスク
Local Name	ローカル側システム名
Remote Name	リモート側システム名
Local port number	ローカル側ポート
Remote port number	リモート側ポート
Transport protocol	トランスポート層プロトコル
DF Bit	外側 IP ヘッダーのフラグメント不可フラグ (DF Bit) の値。COPY (内側のオリジナル IP ヘッダーの値をコピー)、CLEAR (常にオフ)、SET (常にオン) のいずれか
Last sent sequence number	SA が送信した最新パケットのシーケンス番号
Anti-replay checking enabled	リプレイ防止機能の有効・無効
Anti-replay window size	リプレイ防止ウィンドウサイズ
Last received sequence number	SA が受信した最新パケットのシーケンス番号
Anti-replay bitmap	リプレイ防止ウィンドウのビットマップ。ビットマップはリプレイ防止ウィンドウサイズと同じ長さ (以下 n とする) で、過去 n 個分のシーケンス番号を保存している。「1」は該当シーケンス番号のパケットが受信済み、「0」は未受信であることを示す
Debug device	デバッグ情報の出力先デバイス (ポート) 番号
Filter debug flags	フィルタデバッグがオンに設定されているセクターと許可/拒否の結果を示すフラグ
Packet debug flags	パケットデバッグがオンに設定されている処理部とパケットの向きを示すフラグ。パケットの一部も表示される
Trace debug flags	トレースデバッグのオン・オフを示すフラグ
Packet debug length	パケットデバッグ時に表示されるデータ長さ

表 14: SA 指定時

outProcessStart	外向きパケットに対する処理を開始した回数
outProcessFail	外向きパケットに対する処理が失敗した回数
outProcessFailImm	外向きパケットに対する処理が即時失敗した回数
outProcessDone	外向きパケットに対する処理完了回数
espOutBufChainCopy	外向きパケットが ESP 処理のためチェーンからバッファにコピーされた回数
espEncryptionStart	ESP 暗号化処理の開始回数
espEncryptionFail	ESP 暗号化処理の失敗回数
espOutHashStart	外向きパケットに対する ESP 認証処理の開始回数
espOutHashFail	外向きパケットに対する ESP 認証処理の失敗回数
espEncryptionFailImm	ESP 暗号化処理の即時開始回数

espEncryptionGood	ESP 暗号化処理の成功回数
espOutHashFailImm	外向きパケットに対する ESP 認証処理の即時失敗回数
espOutHashGood	外向きパケットに対する ESP 認証処理の成功回数
ahOutBufChainCopy	外向きパケットが AH 処理のためチェーンからバッファにコピーされた回数
ahOutHashStart	外向きパケットに対する AH 認証処理の開始回数
ahOutHashFail	外向きパケットに対する AH 認証処理の失敗回数
ahSeqNumberCycled	AH 認証処理のシーケンスナンバーが一巡した回数
ahOutHashFailImm	外向きパケットに対する AH 認証処理が即時失敗した回数
ahOutHashGood	外向きパケットに対する AH 認証処理の成功回数
compOutBufChainCopy	外向きパケットが IPComp 処理のためチェーンからバッファにコピーされた回数
nonExpansionBackoff	non-expansion backoff のためパケットが圧縮されなかった回数
compressionStart	外向きパケットに対する IPComp 圧縮処理の開始回数
compressionFail	外向きパケットに対する IPComp 圧縮処理の失敗回数
compTooSmall	パケットが小さすぎるため IPComp 圧縮処理が行われなかった回数
dataExpansion	圧縮によってパケットサイズが増大した回数
compressionFailImm	外向きパケットに対する IPComp 圧縮処理が即時失敗した回数
compressionGood	外向きパケットに対する IPComp 圧縮処理の成功回数
inProcessStart	内向きパケットに対する処理開始回数
inProcessFail	内向きパケットに対する処理が失敗した回数
inProcessFailImm	内向きパケットに対する処理が即時失敗した回数
inProcessDone	内向きパケットに対する処理が成功した回数
espInBufChainCopy	内向きパケットが ESP 処理のためチェーンからバッファにコピーされた回数
espInHashStart	内向きパケットに対する ESP 認証処理が開始された回数
espInHashFail	内向きパケットに対する ESP 認証処理が失敗した回数
espDecryptionStart	内向きパケットに対する ESP 復号化処理が開始された回数
espDecryptionFail	内向きパケットに対する ESP 復号化処理が失敗した回数
espIcVInvalid	無効な ICV を持つ ESP パケット受信数
espReplayedPacket	無効なシーケンス番号を持つ ESP パケット受信回数
espInHashFailImm	内向きパケットに対する ESP 認証処理が即時失敗した回数
espInHashGood	内向きパケットに対する ESP 認証処理が成功した回数
espDecryptionFailImm	内向きパケットに対する ESP 復号化処理が即時失敗した回数
espDecryptionGood	内向きパケットに対する ESP 復号化処理が成功した回数
espPaddingInvalid	パディングが無効な ESP パケット受信数
ahInBufChainCopy	内向きパケットが AH 処理のためチェーンからバッファにコピーされた回数

ahBadPayloadLength	無効なペイロード長を持つ AH パケット受信数
ahInHashStart	内向きパケットに対する AH 認証処理の開始回数
ahInHashFail	内向きパケットに対する AH 認証処理の失敗回数
ahReplayedPacket	無効なシーケンス番号を持つ AH パケット受信回数
ahIcVInvalid	無効な ICV を持つ AH パケット受信数
ahInHashFailImm	内向きパケットに対する AH 認証処理の即時失敗回数
ahInHashGood	内向きパケットに対する AH 認証処理の成功回数
compInBufChainCopy	内向きパケットが IPComp 処理のためチェーンからバッファにコピーされた回数
decompressionStart	内向きパケットに対する IPComp 圧縮解除処理の開始回数
decompressionFail	内向きパケットに対する IPComp 圧縮解除処理の失敗回数
decompressionFailImm	内向きパケットに対する IPComp 圧縮解除処理の即時失敗回数
decompressionGood	内向きパケットに対する IPComp 圧縮解除処理の成功回数

表 15: COUNTER オプション指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

SHOW IPSEC（88 ページ）

SHOW IPSEC SASPECIFICATION

カテゴリー：IPsec / SA スペック

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW IPSEC SASPECIFICATION [=saspec-id]

saspec-id: SA スペック番号 (0~255)

解説

SA スペックに関する情報を表示する。

パラメーター

SASPECIFICATION SA スペック番号。省略時はすべての SA スペックの情報を簡潔に表示する。指定時は該当する SA スペックの詳細情報を表示する。

入力・出力・画面例

```
SecOff > show ipsec saspecification
```

ID	Proto	KeyMan	Mode	EncAlg	HashAlg	CompAlg	InSpi	EncKey	HashKey
1	COMP	ISAKMP	-	NULL	NULL	LZS	-	-	-
2	ESP	ISAKMP	TUNNEL	DES	MD5	-	-	-	-

```
SecOff > show ipsec saspecification=2
```

Sa Specification

```

Id ..... 2
Protocol ..... ESP
Key Management ..... ISAKMP
Mode ..... TUNNEL
Encryption Algorithm ..... DES
Hash Algorithm ..... MD5
Compression Algorithm ..... -
In SPI ..... -
Out SPI ..... -
Encryption Key ..... -
Hash Key ..... -
AntiReplay Enabled ..... FALSE
Replay Window Size ..... 32

```

ID	SA スペック番号
Protocol	IPsec セキュリティープロトコル。ESP (暗号化ペイロード) \ AH (認証ヘッダー) \ COMP (IPComp、IP 圧縮) のいずれか
KeyMan	鍵管理方式。MANUAL (手動) または ISAKMP (自動)
Mode	SA 動作モード。TUNNEL (トンネルモード) か TRANSPORT (トランスポートモード)
EncAlg	ESP が使う暗号化アルゴリズム
HashAlg	AH と ESP が使う認証用ハッシュアルゴリズム
CompAlg	IPComp が使う圧縮アルゴリズム
InSpi	内向きトラフィックの SPI (Security Parameter Index)
EncKey	暗号鍵番号
HashKey	認証用ハッシュ鍵番号

表 16: SA スペック無指定時

Id	SA スペック番号
Protocol	IPsec セキュリティープロトコル。ESP (暗号化ペイロード) \ AH (認証ヘッダー) \ COMP (IPComp、IP 圧縮) のいずれか
Key Management	鍵管理方式。MANUAL (手動) または ISAKMP (自動)
Mode	SA 動作モード。TUNNEL (トンネルモード) か TRANSPORT (トランスポートモード)
Encryption Algorithm	ESP が使う暗号化アルゴリズム
Hash Algorithm	AH と ESP が使う認証用ハッシュアルゴリズム
Compression Algorithm	IPComp が使う圧縮アルゴリズム
In SPI	内向きトラフィックの SPI (Security Parameter Index)
Out SPI	外向きトラフィックの SPI (Security Parameter Index)
Encryption Key	暗号鍵番号
Hash Key	認証用ハッシュ鍵番号
AntiReplay Enabled	リプレイ防止機能の有効 (TRUE) \ 無効 (FALSE)
Replay Window Size	リプレイ防止ウィンドウサイズ。32、64、128、256 のいずれか

表 17: SA スペック指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

CREATE IPSEC SASPECIFICATION (43 ページ)

DESTROY IPSEC SASPECIFICATION (51 ページ)

SET IPSEC SASPECIFICATION (81 ページ)

SHOW ISAKMP

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW ISAKMP

解説

ISAKMP モジュールの情報を表示する。

入力・出力・画面例

```
SecOff > show isakmp

ISAKMP Module Configuration

Module Status ..... ENABLED
UDP Port ..... 500
Debug Flag ..... 00000000
Global Debug Device ..... 0
Local RSA Key ..... -
VPN Client Policy Server Enabled ..... FALSE
VPN Client Policy File Name .....
```

Module Status	ISAKMP モジュールの有効・無効
UDP Port	ISAKMP メッセージの送受信に使う UDP ポート
Debug Flag	各デバッグオプションの有効・無効を示すビット列。数字は一番左から、パケットデバッグ（第 0 ビット）、状態遷移デバッグ（第 1 ビット）、トレースデバッグ（第 3 ビット）。値 0 は無効、値 1 は有効
Global Debug Device	デバッグ情報の出力先ポート番号
Local RSA key	デフォルトの RSA 秘密鍵番号
VPN Client Policy Server Enabled	セキュリティポリシーサーバー機能の有効・無効
VPN Client Policy File Name	クライアントに送信するデフォルトのセキュリティポリシーファイル名

表 18:

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

DISABLE ISAKMP (56 ページ)

ENABLE ISAKMP (62 ページ)

SHOW ISAKMP COUNTERS

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW ISAKMP COUNTERS [= {GENERAL|MAIN|QUICK|SAD|SPD|XDB|IPSEC|INFO|
AGGRESSIVE|NETWORK|TRANSACTION}]

解説

ISAKMP モジュールのデバッグ用統計カウンターを表示する。

パラメーター

COUNTERS 統計カウンターのカテゴリーを指定する。省略時はすべてのカウンターが表示される。

入力・出力・画面例

```
SecOff > show isakmp counters=general
```

ISAKMP General Counters

acquire	6		
acquireNoPolicy	0	acquireNoSa	3
acquireEquivFound	0	acqPh2EquivInProgress	3
acqPh1XchgStartFailed	0	acqPh2XchgStartFailed	0
acquireQueued	3	acqPeerAddrNameIncons	0
acquirePrenegNoPolicy	0		
msgInitPhlp5StartFail	0		
doneGood	6	donePhase1Failed	0
doneSendConNoSa	0		
msgTx	15	msgTxd	15
txEncryptNoExchange	0	msgTxEncryptNoEncoProc	0
msgTxStartEncrypt	9		
txEncryptFail	0	txEncryptGood	9
msgTxEncryptExpKBytes	0		
txRetryTxd	0	txRetryXchgTimedOut	0
msgRxd	12		
msgRxInconsistLengths	0	msgRxBadLength	0
msgRxBadReserved	0	msgRxBadVersion	0
msgRxBadNextPayload	0	msgRxUnexpectedMsg	0

msgRxNoExchange	0	msgRxNoExchangePhase1	0
msgRxPlNoXcgNot1stMsg	0	msgRxPh1UnkwnXchgType	0
msgRxPh1XchgStartFail	0	msgRxPh1MsgIdNotZero	0
msgRxPl5XchgStartFail	0		
msgRxPhase2NoSa	0	msgRxNoExchangePhase2	0
msgRxPh2XchgStartFail	0	msgRxPh2UnkwnXchgType	0
msgRxEncrypted	6	msgRxEncryptdUnexpect	0
msgRxBadPad	0	msgRxBadPadLength	0
msgRxPayBadNextPay	0	msgRxPayBadReserved	0
msgRxDecryptNoEncoPrc	0	msgRxStartDecrypt	6
msgRxPlain	6	msgRxPlainUnexpected	0
rxDecryptNoExchange	0	rxDecryptBadLength	0
rxDecryptGood	6	rxDecryptFail	0
rxDecryptBadPad	0	rxDecryptBadPadLength	0
rxDecrptPayBadNextPay	0	rxDecryptPayBadRsvd	0
infoNoMatchingPolicy	0	infoPh1NotifyDisabled	0
infoPh1NoDelAllowed	0	infoPh1ExchgStartFail	0
infoPh2SASNotFound	4	infoPh2SASNotActive	0
infoPh2NotifyDisabled	0	infoPh2DeleteDisabled	0
infoPh2XchgStartFail	0		

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

SHOW ISAKMP EXCHANGE（118 ページ）

SHOW ISAKMP SA（126 ページ）

SHOW ISAKMP EXCHANGE

カテゴリー：IPsec / ISAKMP
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW ISAKMP EXCHANGE[=*exchange-id*]

exchange-id: ISAKMP Exchange 番号 (0 ~ 65535)

解説

ISAKMP 交換 (一連のメッセージ交換) の情報を表示する。

パラメーター

EXCHANGE ISAKMP Exchange 番号

入力・出力・画面例

SecOff > sh isakmp exchange				
ISAKMP Exchanges				
Id	Phase	State	PeerAddress	Type

7	1	SASENT	1.1.1.1	MAIN

Id	ISAKMP 交換 ID
Phase	ISAKMP フェーズ。1、1.5、2 のいずれか
State	交換の状態。Main モード (Identity Protection 交換) では IDLE、SASENT、SARECV、KESENT、KEREVC、AUTHSENT、AUTHRECV、UP のいずれか。Quick モードでは、STARTING、WAIT_HASH_SA_NONCE、WAIT_HASH、RECEIVING_MESSAGE、SENDING_HASH_SA_NONCE、SENDING_HASH、DONE のいずれか。Aggressive モード (Aggressive 交換) では、IDLE、SAKESNT、SAKERECV、SAKEAUTHSENT、SAKEAUTHRECV、AUTHSENT、AUTHRECV、UP のいずれか。Transaction 交換では、IDLE、REQSENT、REQRECV、REPRESENT、REPRECV、SETSENT、SETRECV、ACKSENT、ACKRECV、UP のいずれか。Informational 交換では IDLE となる

Peer Address/Peer IP Address	ISAKMP ピアの IP アドレス
Type	交換タイプ。MAIN、AGGRESSIVE、TRANSACTION、INFO、QUICK のいずれか

表 19: Exchange 番号無指定時

ISAKMP Exchange	交換に関する一般情報
Id	ISAKMP 交換 ID
Phase	ISAKMP フェーズ。1、1.5、2 のいずれか
State	交換の状態。Main モード (Identity Protection 交換) では IDLE、SASENT、SARECV、KESENT、KERECV、AUTH-SENT、AUTHRECV、UP のいずれか。Quick モードでは、STARTING、WAIT_HASH_SA_NONCE、WAIT_HASH、RECEIVING_MESSAGE、SENDING_HASH_SA_NONCE、SENDING_HASH、DONE のいずれか。Aggressive モード (Aggressive 交換) では、IDLE、SAKASENT、SAKERECV、SAKEAUTHSENT、SAKEAUTHRECV、AUTHSENT、AUTHRECV、UP のいずれか。Transaction 交換では、IDLE、REQSENT、REQRECV、REPSSENT、REPRECV、SETSENT、SETRECV、ACKSENT、ACKRECV、UP のいずれか。Informational 交換では IDLE となる
Type	交換タイプ。MAIN、AGGRESSIVE、TRANSACTION、INFO、QUICK のいずれか
Initiator	始動者 (イニシエーター)・応答者 (レスポnder) の区別
DOI	DOI (Domain Of Interpretation)、IPsec のみサポート
Policy name	ISAKMP ポリシー名
SA	ISAKMP SA 番号
Peer Address/Peer IP Address	ISAKMP メッセージのリモート側 IP アドレス
Local IP Address	ISAKMP メッセージのローカル側アドレス
Encrypted	ISAKMP SA による保護が提供されているかどうか
Expecting message	新しいメッセージを待っているかどうか
Has SA	ISAKMP SA が確立されているかどうか
Initiator Cookie	始動者クッキー。交換を開始した側が生成した 8 バイトの乱数値
Responder Cookie	応答者クッキー。交換の応答側が生成した 8 バイトの乱数値
Message Id	フェーズ 2 交換を識別するために用いられる 4 バイトの乱数値
Set Commit bit	送信時に ISAKMP ヘッダーの Commit ビットを立てるかどうか
Commit bit received	受信メッセージの Commit ビットが立っているかどうか
Send notifies	Notify ペイロードを送信するかどうか

Send deletes	Delete ペイロードを送信するかどうか
Message Retry Limit	メッセージの最大再送回数
Packet Retry Counter	現在送信中のメッセージの残り再送回数
Initial Message Retry Timeout (s)	初回送信時の再送待ち時間 (秒)
Packet Retry Timer (time left(s))	現在送信中のメッセージを再送するまでの残り時間 (秒)
Main and Aggressive Mode	Main モードと Aggressive モードに関する情報が表示される
ENCO Pass	ENCO モジュールによる「パス」回数
Shared Key Id	事前共有鍵 (PRESHARED) 認証で用いる共有鍵番号
Peer RSA Key Id	公開鍵暗号 (RSAENCR) 認証で用いる相手の RSA 公開鍵番号
Local RSA Key Id	自分の RSA 公開鍵ペア番号
Peer Certificate Id	相手の証明書 ID
Local Certificate Id	自分の証明書 ID
Local Policy	自分のポリシー
Remote Policy	相手のポリシー
Transform	Transform ペイロードに関する情報が表示される
Transform Number	SA ペイロードに含まれる Transform ペイロードの数
Transform Id	Transform ペイロード ID
Encryption Algorithm	暗号化アルゴリズム
Authentication Algorithm	認証アルゴリズム
Authentication Method	フェーズ 1 の相手認証方式。事前共有鍵 (PRESHARED)、公開鍵暗号 (RSAENCR)、デジタル署名 (RSASIG) のいずれか
Group Description	Diffie-Hellman (Oakley) グループ番号。MODP768、MODP1024、INVALID、NONE のいずれか
Group Type	Diffie-Hellman (Oakley) グループタイプ
DH Private Exponent Bits	DH 秘密べき乗数のビット長
Expiry Seconds	自分のポリシーで指定された SA の有効期限 (秒)
Expiry KBytes	自分のポリシーで指定された SA の有効期限 (キロバイト)
Transaction Mode	Transaction 交換に関する情報が表示される
Mode	Transaction 交換モード。XAUTH、SET、REQ のいずれか
Id	交換 ID
Quick Mode Status	Quick モードに関する情報が表示される
SA id	ISAKMP SA の ID
local address	ローカル側 IP アドレス
policy name	ISAKMP ポリシー名
use PFS-KEY	Perfect Forward Security for keys を使用するかどうか
use PFS-ID	Perfect Forward Security for IDs を使用するかどうか
DH group ID	Diffie-Hellman (Oakley) グループ ID
msg retry limit	メッセージの最大再送回数

msg retry timeout	メッセージの初回送信時から最初の再送までの時間 (秒)
IPSEC exchange info	IPsec 関連情報が表示される
IDi	始動者 ID に関する情報
type	ID タイプ
protocol Id	プロトコル ID
port	ポート ID
data	ID データ
IDr	応答者 ID に関する情報
group Id	IPsec グループ ID
Sa Definition Information	SA 定義に関する情報が表示される
Authentication Type	SA の認証方式
Encryption Algorithm	SA の暗号化アルゴリズム
Hash Algorithm	SA の認証用ハッシュアルゴリズム
group Type	Diffie-Hellman (Oakley) グループタイプ
group Description	Diffie-Hellman (Oakley) グループ
expiry seconds	ネゴシエートされた SA の有効期限 (秒)
expiry kilobytes	ネゴシエートされた SA の有効期限 (キロバイト)

表 20: Exchange 番号指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

SHOW ISAKMP COUNTERS (116 ページ)

SHOW ISAKMP SA (126 ページ)

SHOW ISAKMP POLICY

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW ISAKMP POLICY[=*policy*]

policy: ISAKMP ポリシー名 (1～24 文字)

解説

ISAKMP ポリシーに関する情報を表示する。

パラメーター

POLICY ISAKMP ポリシー名

入力・出力・画面例

```
SecOff > show isakmp policy
```

```
ISAKMP Policies
```

Name	Mode	AuthType	EncAlg	HashAlg	PeerAddress
i	IDPROT	PRESHARED	DES	SHA	1.1.1.1

```
SecOff > show isakmp policy=i
```

```
ISAKMP Policy
```

```

Name ..... i
Peer Address ..... 1.1.1.1
Peer Port ..... 500
Phase1 Mode ..... IDPROT
Authentication Type ..... PRESHARED
Extended Authentication ..... NONE
Extended Authentication Type ..... -
Extended Authentication User Name ..... -
Extended Authentication Password ..... -
Key Id ..... 1
Local RSA key ..... -
Phase 2 Exchanges Limit ..... NONE
PreNegotiate ..... FALSE
DOI ..... IPSEC
SendNotify Messages ..... TRUE
Send Delete Messages ..... FALSE

```

Always Send ID Messages	FALSE
Commit Bit	FALSE
Message Retry Limit	5
Message Time Out	20
Source Interface	-
Local ID	FQDN:client
Remote ID	-
VPN Client Policy File Name	-
DebugFlag	00000000
SA Specification	
Encryption Algorithm	DES - 56 bit
Hash Algorithm	SHA
Group Description	1
DH Private Exponent Bits	160
Heartbeat Mode	NONE
Group Type	MODP
Expiry Seconds	86400
Expiry Kilobytes	-

Name	ISAKMP ポリシー名
Mode	フェーズ1 モード。IDPROT (Main モード) か AGGR (Aggressive モード)
AuthType	フェーズ1 の相手認証方式。事前共有鍵 (PRESHARED)、公開鍵暗号 (RSAENCR)、デジタル署名 (RSASIG) のいずれか
EncAlg	ISAKMP SA が使用する暗号アルゴリズム
HashAlg	ISAKMP SA が使用する認証用ハッシュアルゴリズム
PeerAdresss	ISAKMP ピアの IP アドレス。ANY は IP アドレスが不定であることを示す

表 21: 無指定時

Name	ISAKMP ポリシー名
Peer Adresss	ISAKMP ピアの IP アドレス。ANY は IP アドレスが不定であることを示す
Phase1 Mode	フェーズ1 モード。IDPROT (Main モード) か AGGR (Aggressive モード)
Authentication Type	フェーズ1 の相手認証方式。事前共有鍵 (PRESHARED)、公開鍵暗号 (RSAENCR)、デジタル署名 (RSASIG) のいずれか
Extended Authentication	拡張認証 (XAUTH) における役割。CLIENT (認証を受ける側)、SERVER (認証する側)、NONE (XAUTH を使わない) のいずれか
Extended Authentication Type	拡張認証 (XAUTH) 方式。RADIUS_CHAP、GENERIC のいずれか

Extended Authentication User Name	XAUTH のクライアントユーザー名
Extended Authentication Password	XAUTH のクライアントパスワード
Key Id	認証鍵番号
Local RSA key	自分の RSA 鍵番号
Peer Certificate Id	相手の公開鍵証明書 ID
Phase 2 Exchanges Limit	ISAKMP SA 上で実行が許されるフェーズ 2 交換の最大数。 フェーズ 2 交換の回数がこの値を超えると、ISAKMP SA が 再ネゴシエートされる
PreNegotiate	ルーター起動時に ISAKMP SA のネゴシエーションを行っ ておくかどうか
DOI	ISAKMP ポリシーの DOI (Domain of Interpretation)。 IPSEC のみサポート
Send Notify Messages	Notify ペイロードの送信を許可するか
Send Delete Messages	Delete ペイロードの送信を許可するか
Always Send ID Messages	ISAKMP SA のネゴシエート時に必ず ID ペイロードを送信 するか
Commit Bit	メッセージ送信時に Commit ビットをセットするかどうか
Message Retry Limit	ISAKMP メッセージの最大再送回数
Message Time Out	ISAKMP メッセージの再送間隔
Source Interface	ISAKMP メッセージの始点インターフェース。このインター フェースの IP アドレスが始点アドレスとなる
DebugFlag	有効な ISAKMP デバッグオプションを示すフラグ
SA Specification	SA スペックに関する情報が表示される
Encryption Algorithm	ISAKMP SA が使用する暗号アルゴリズム
Hash Algorithm	ISAKMP SA が使用する認証用ハッシュアルゴリズム
Group Description	Diffie-Hellman (Oakley) グループ番号。1 か 2
DH Private Exponent Bits	DH 秘密べき乗数のビット長
Group Type	Diffie-Hellman (Oakley) グループタイプ。MODP のみサ ポート
Expiry Seconds	ISAKMP SA の有効期限 (秒)
Expiry Kilobytes	ISAKMP SA の有効期限 (キロバイト)

表 22: 指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード (AR010) または暗号・圧縮ボード (AR011) を装着する必要がある。

関連コマンド

SHOW ISAKMP (114 ページ)

SHOW ISAKMP COUNTERS (116 ページ)

SHOW ISAKMP SA

カテゴリー：IPsec / ISAKMP

対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW ISAKMP SA [=sa-id]

sa-id: SA 番号 (0 ~ 65535)

解説

ISAKMP SA に関する情報を表示する。

パラメーター

SA SA 番号

入力・出力・画面例

```
SecOff > show isakmp sa
```

SA Id	PeerAddress	EncA.	HashA.	Bytes	Expiry Limits - hard/soft/used Seconds
3	1.1.1.1	DES	SHA	-/-/-	86400/82080/538

```
SecOff > show isakmp sa=3
```

```
SA Id ..... 3
Initiator Cookie ..... c551ea94cc152a8d
Responder Cookie ..... 9b7bf67d53e85104
DOI ..... IPSEC
Policy name ..... i
State ..... ACTIVE
Local address ..... 63.12.66.239
Remote Address ..... 1.1.1.1
Remote Port ..... 500
Time of establishment ..... 03-Oct-2001:11:54:05
Commit bit set ..... FALSE
Send notifies ..... TRUE
Send deletes ..... FALSE
Always send ID ..... FALSE
Message Retry Limit ..... 5
Initial Message Retry Timeout (s) ... 20
Do Xauth ..... FALSE
Xauth Finished ..... TRUE
```

Expiry Limit (bytes)	-
Soft Expiry Limit (bytes)	-
Bytes seen	-
Expiry Limit (seconds)	86400
Soft Expiry Limit (seconds)	82080
Seconds since creation	549
Number of Phase 2 exchanges allowed .	4294967294
Number of acquires queued	0
Sa Definition Information:	
Authentication Type	PRESHARED
Encryption Algorithm	DES - 56 bit
Hash Algorithm	SHA
group Type	MODP
group Description	MODP768
DH Private Exponent Bits	160
expiry seconds	86400
expiry kilobytes	-
XAuth Information:	
Id	0
Next Message	UNKNOWN
Status	FAIL
Type	Generic
Max Failed Attempts.....	0
Failed Attempts.....	0
Heartbeat information:	
Send Heartbeats	NO
Next sequence number tx	1
Receive Heartbeats	NO
Last sequence number rx	0

SA Id	SA ID
PeerAddress	SA のリモート側 IP アドレス
EncA	SA の暗号化アルゴリズム
HashA	SA の認証ハッシュアルゴリズム
Bytes	SA の有効期限 (バイト)。ハードリミット (SA 削除までの期限) ソフトリミット (SA 再ネゴシエートまでの期限) 現在までに処理されたバイト数の順に表示される
Seconds	SA の有効期限 (秒)。ハードリミット (SA 削除までの期限) ソフトリミット (SA 再ネゴシエートまでの期限) 現在までに経過した秒数の順に表示される

表 23: 無指定時

SA Id	SA ID
-------	-------

Initiator Cookie	始動者クッキー
Responder Cookie	応答者クッキー
DOI	DOI (Domain Of Interpretation)、IPSEC のみサポート
Policy name	ISAKMP ポリシー名
State	ISAKMP SA の状態。ACTIVE、EXPIRED、DOING、NEW_GROUP、DOING_XAUTH のいずれか
Local Address	SA のローカル側 IP アドレス
Remote Address	SA のリモート側 IP アドレス
Time of establishment	SA の作成日時
Commit bit set	Commit ビットがセットされているかどうか
Send notifies	Notify ペイロードを送信するか
Send deletes	Delete ペイロードを送信するか
Message Retry Limit	メッセージの最大再送回数
Initial Message Retry Timeout (s)	メッセージの初回送信時から最初の再送までの時間 (秒)
Do Xauth	XAUTH 認証を使うかどうか
Xauth Finished	XAUTH 認証が完了したかどうか
Expiry Limit (bytes)	SA の有効期限 (バイト数)、SA 削除までの期限 (ハードリミット)
Soft Expiry Limit (bytes)	SA の有効期限 (バイト数)、再ネゴシエートまでの期限 (ソフトリミット)
Bytes seen	現在までに SA が処理したバイト数
Expiry Limit (seconds)	SA の有効期限 (秒)、SA 削除までの期限 (ハードリミット)
Soft Expiry Limit (seconds)	SA の有効期限 (秒)、再ネゴシエートまでの期限 (ソフトリミット)
Seconds since creation	SA 作成後の経過時間 (秒)
Number of Phase 2 exchanges allowed	この SA 上で実行可能なフェーズ 2 交換の最大数
Number of acquires queued	処理待ちの IPSEC SA ネゴシエーション要求数
Sa Definition Information	SA 定義に関する情報が表示される
Authentication Type	相手認証方式
Encryption Algorithm	SA の暗号アルゴリズム
Hash Algorithm	SA の認証用ハッシュアルゴリズム
group Type	Diffie-Hellman (Oakley) グループタイプ
group Description	Diffie-Hellman (Oakley) グループ
DH Private Exponent Bits	DH 秘密べき乗数のビット長
expiry seconds	ネゴシエートされた SA の有効期限 (秒)
expiry kilobytes	ネゴシエートされた SA の有効期限 (キロバイト)
XAuth Information	XAUTH に関する情報が表示される

Id	XAUTH 認証のメッセージ ID
Next Message	次に送信される XAUTH メッセージ。REQ か SET のいずれか
Status	XAUTH 認証の状態。OK か FAIL のいずれか
Type	XAUTH 認証のタイプ。GENERIC か RADIUS-CHAP のいずれか
Max Failed Attempts	XAUTH 認証の最大試行回数。この回数を超過して失敗すると SA が削除される
Failed Attempts	XAUTH 認証の失敗回数

表 24: 指定時

備考・注意事項

IPsec を使用するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要がある。

関連コマンド

SHOW ISAKMP COUNTERS (116 ページ)

SHOW ISAKMP EXCHANGE (118 ページ)