IPsec データ プレーンの設定ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

IPsec アンチ リプレイ ウィンドウの拡張と無効化 3

機能情報の確認 3

IPsec アンチ リプレイ ウィンドウの拡張と無効化の前提条件 4

IPsec アンチ リプレイ ウィンドウの拡張と無効化に関する情報 4

IPsec アンチ リプレイ ウィンドウ 4

IPsec アンチ リプレイ ウィンドウの拡張と無効化機能の設定方法 5

IPsec アンチ リプレイ ウィンドウの拡張と無効化のグローバル設定 5

暗号マップ上における IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定 6

トラブルシューティングのヒント 7

IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定例 7

アンチ リプレイ ウィンドウのグローバル拡張と無効化：例 7

暗号マップまたは暗号プロファイルのアンチ リプレイ ウィンドウの拡張および無効化：例 8

その他の参考資料 9

IPsec アンチ リプレイ ウィンドウの拡張と無効化の機能情報 11

IPsec VPN の Pre-fragmentation 13

機能情報の確認 13

IPsec VPN の Pre-fragmentation の制約事項 13

IPsec VPN の Pre-fragmentation に関する情報 15

IPsec VPN の Pre-fragmentation 15

IPsec VPN の Pre-fragmentation の設定方法 16

IPsec VPN の Pre-fragmentation の設定 16

その他の参考資料 17

IPsec VPN の Pre-fragmentation の機能情報 18

Invalid Security Parameter Index Recovery 21

機能情報の確認 21

Invalid Security Parameter Index Recovery の前提条件 22
Invalid Security Parameter Index Recovery の制約事項 22
Invalid Security Parameter Index Recovery に関する情報 22
機能の動作 22
Invalid Security Parameter Index Recovery の設定方法 23
Invalid Security Parameter Index Recovery の設定 23
事前共有設定の確認 24
Invalid Security Parameter Index Recovery の設定例 29
Invalid Security Parameter Index Recovery：例 29
その他の参考資料 34
関連資料 34
標準 34
MIB 34
RFC 35
シスコのテクニカル サポート 35
Invalid Security Parameter Index Recovery の機能情報 35
IPSec デッド ピア検出定期メッセージ オプション 37
機能情報の確認 37
IPSec デッド ピア検出定期メッセージ オプションの前提条件 38
IPSec デッド ピア検出定期メッセージ オプションの制約事項 38
IPSec デッド ピア検出定期メッセージ オプションに関する情報 38
DPD および Cisco IOS XE キープアライブ機能の動作 38
IPSec デッド ピア検出定期メッセージ オプションの使用 39
暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブ機能の使用 39
Easy VPN Remote コンフィギュレーション内での DPD の使用 39
IPSec デッド ピア検出定期メッセージ オプションの設定方法 40
定期的な DPD メッセージの設定 40
暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブの設定 41
Easy VPN Remote の DPD の設定 43
DPD が有効化されていることの確認 44
IPSec デッド ピア検出定期メッセージ オプションの設定例 45

定期的な DPD を有効化したサイト間設定の例 45
DPD を有効化した Easy VPN Remote の例 46
debug crypto isakmp コマンドを使用した DPD 設定の確認の例 46
暗号マップ内の複数のピアとの組み合わせで使用される DPD および Cisco IOS XE キープアライブ：例 48
Easy VPN Remote の複数のピアとの組み合わせで使用される DPD の例 49
その他の参考資料 49
関連資料 49
標準 49
MIB 50
RFC 50
シスコのテクニカル サポート 50
デッド ピア検出定期メッセージ オプションの機能情報 51
IPsec NAT 透過性 53
機能情報の確認 53
IPsec NAT 透過性の制約事項 54
IPsec NAT 透過性に関する情報 54
IPsec NAT 透過性の利点 54
IPsec NAT Traversal の機能設計 54
IKE フェーズ 1 ネゴシエーション：NAT 検出 54
IKE フェーズ 2 ネゴシエーション：NAT トラバーサル決定 55
NAT Traversal 用 IPsec パケットの UDP カプセル化 55
IPsec ESP と PAT との間における非互換性：解決 55
チェックサムと NAT との間における非互換性：解決 56
固定 IKE 宛先ポートおよび PAT 間における非互換性：解決 56
ソフトウェア エンジン用 UDP カプセル化処理：トランスポート モードおよびトンネル モード EDP カプセル化 58
NAT キープアライブ 58
NAT および IPsec の設定方法 59
NAT Traversal の設定 59
NAT Traversal の無効化 59
NAT キープアライブの設定 60
IPsec 設定の確認 61

IPsec および NAT の設定例 62
NAT キープアライブの設定例 62
その他の参考資料 62
IPsec NAT 透過性の機能情報 64
用語集 65
IPsec トンネルを使用する DF ビット オーバーライド機能 67
機能情報の確認 67
IPsec トンネルを使用する DF ビット オーバーライド機能の前提条件 68
IPsec トンネルを使用する DF ビット オーバーライド機能の制約事項 68
IPsec トンネルを使用する DF ビット オーバーライド機能に関する情報 68
機能の概要 68
IPsec トンネルを使用する DF ビット オーバーライド機能の設定方法 69
トンネル モードでのカプセル化ヘッダーへの DF ビットの設定 69
DF ビット設定の確認 70
IPsec トンネルを使用する DF ビット オーバーライド機能の設定例 70
DF ビットの設定例 70
その他の参考資料 71
関連資料 71
標準 71
MIB 72
RFC 72
シスコのテクニカル サポート 72
IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報 73
IPsec SA アイドル タイマー 75
機能情報の確認 75
IPsec セキュリティ アソシエーション アイドル タイマーの前提条件 76
IPsec セキュリティ アソシエーション アイドル タイマーに関する情報 76
IPsec セキュリティ アソシエーションのライフタイム 76
IPsec SA アイドル タイマー 76
IPsec セキュリティ アソシエーション アイドル タイマーの設定方法 77
IPSec SA アイドル タイマーのグローバルな設定 77
IPSec SA アイドル タイマーのクリプト マップ単位での設定 78
IPsec セキュリティ アソシエーション アイドル タイマーの設定例 79

IPsec SA アイドル タイマー のグローバル設定例 79
暗号マップごとの IPsec SA アイドル タイマーの設定例 79
その他の参考資料 79
IPsec セキュリティ アソシエーション アイドル タイマーの機能仕様 81
IPv6 IPsec の QoS 83
機能情報の確認 83
IPv6 IPsec QoS に関する情報 84
IPv6 IPsec QoS の概要 84
IPv6 IPsec QoS の設定方法 84
Crypto LLQ QoS の設定 84
QoS Pre-classify の設定 86
暗号マップ上での Pre-classify の設定 86
トンネル インターフェイス上での Pre-classify の設定 87
LLQ QoS グループの設定 88
QoS の設定例 89
例：Crypto LLQ QoS の設定 89
例：暗号マップ上での Pre-classify の設定 90
例：トンネル インターフェイス上での Pre-classify の設定 90
例：LLQ QoS グループの設定 90
IPv6 IPsec QoS の追加情報 91
IPv6 IPsec QoS の機能情報 92
IPv6 仮想トンネル インターフェイス 93
機能情報の確認 93
IPv6 仮想トンネル インターフェイスに関する情報 94
IPsec for IPv6 94
仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護 95
IPv6 仮想トンネル インターフェイスの設定方法 96
サイト間 IPv6 IPsec 保護用の VTI の設定 96
IPv6 での IKE ポリシーおよび事前共有キーの定義 96
ISAKMP アグレッシブ モードの設定 99
IPsec トランスフォーム セットおよび IPsec プロファイルの定義 100
IPv6 での ISAKMP プロファイルの定義 102

IPv6 IPsec VTI の設定 **103**
IPsec トンネル モード設定の確認 **105**
IPsec for IPv6 の設定と動作のトラブルシューティング **107**
IPv6 仮想トンネル インターフェイスの設定例 **108**
例：サイト間 IPv6 IPsec 保護用の VTI の設定 **108**
その他の参考資料 **109**
IPv6 仮想トンネル インターフェイスの機能情報 **110**

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な 2 つのリリースとしての Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）が、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと展開（マージ）されています。これにより、スイッチングおよびルーティング ポートフォリオの広範なアクセスおよびエッジ製品が盛り込まれた 1 つのリリースが実現しました。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術的構成ガイドが製品のランディング ページに表示される場合は、その機能がお使いのプラットフォームでサポートされていることを示します。

第 2 章

IPsec アンチ リプレイ ウィンドウの拡張と無効化

Cisco IP セキュリティ（IPsec）認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます。それらの番号に基づいて、デクリプタが検知したパケットを追跡します。現在、デフォルトのウィンドウサイズは、64パケットです。一般的にはこの数字（ウィンドウ サイズ）で十分ですが、このウィンドウ サイズを拡張する必要がある場合もあります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウサイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

- 機能情報の確認，3 ページ
- IPsec アンチ リプレイ ウィンドウの拡張と無効化の前提条件，4 ページ
- IPsec アンチ リプレイ ウィンドウの拡張と無効化に関する情報，4 ページ
- IPsec アンチ リプレイ ウィンドウの拡張と無効化機能の設定方法，5 ページ
- IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定例，7 ページ
- その他の参考資料，9 ページ
- IPsec アンチ リプレイ ウィンドウの拡張と無効化の機能情報，11 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPsec アンチ リプレイ ウィンドウの拡張と無効化の前提条件

- この機能を設定する前に、クリプトマップまたは暗号プロファイルを作成しておく必要があります。
- IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を設定するには、次の概念を理解しておく必要があります。 IPsec アンチ リプレイ ウィンドウ, （4 ページ）

IPsec アンチ リプレイ ウィンドウの拡張と無効化に関する情報

IPsec アンチ リプレイ ウィンドウ

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチ リプレイ保護が提供されます（セキュリティ アソシエーション（SA）アンチリプレイは、受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービスです）。復号機能によって、以前に認識したシーケンス番号が除外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X（N はウィンドウ サイズ）までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットが廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、Cisco Quality of Service（QoS）によって、ハイプライオリティ パケットにプライオリティが与えられている場合、一部のロープライオリティ パケットが、それらがデクリプタによって受信された最新の 64 パケットの 1 つにもかかわらず、廃棄されてしまう可能性があります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

アンチリプレイ ウィンドウサイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

IPsec アンチ リプレイ ウィンドウの拡張と無効化機能の設定方法

IPsec アンチ リプレイ ウィンドウの拡張と無効化のグローバル設定

IPsec アンチ リプレイ ウィンドウ：拡張と無効化をグローバルに設定する（その結果、作成されるすべての SA が影響を受けます）には、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoipsecsecurity-associationreplaywindow-size** [*N*]
4. **cryptoipsecsecurity-associationreplaydisable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoipsecsecurity-associationreplaywindow-size** [*N*] 例： `Router (config)# crypto ipsec security-association replay window-size 256`	SA リプレイ ウィンドウのサイズをグローバルに設定します。 （注） このコマンドまたは **cryptoipsecsecurity-associationreplaydisable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 4	**cryptoipsecsecurity-associationreplaydisable** 例： `Router (config)# crypto ipsec security-association replay disable`	検査をグローバルにイネーブルにします。 （注） このコマンドまたは **cryptoipsecsecurity-associationreplaywindow-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

	コマンドまたはアクション	目的

暗号マップ上における IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定

暗号マップ上で IPsec アンチ リプレイ ウィンドウの拡張と無効化を、特定の暗号マップまたはプロファイルを使用して作成された SA に影響を与えるように設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptomap***map-nameseq-num* [**ipsec-isakmp**]
4. **setsecurity-associationreplaywindow-size[***N***]**
5. **setsecurity-associationreplaydisable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptomap***map-nameseq-num* [**ipsec-isakmp**] 例： `Router (config)# crypto map ETHO 17 ipsec-isakmp`	クリプトマップ コンフィギュレーション モードを開始し、動的に作成されるクリプトマップの設定のためのテンプレートを提供する暗号プロファイルを作成します。

	コマンドまたはアクション	目的
ステップ 4	**setsecurity-associationreplaywindow-size[*N*]** 例： `Router (crypto-map)# set security-association replay window-size 128`	特定のクリプトマップ、ダイナミック クリプトマップ、または暗号プロファイルによって指定されたポリシーを使用して作成される SA を制御します。 （注） このコマンドまたは **set security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 5	**setsecurity-associationreplaydisable** 例： `Router (crypto-map)# set security-association replay disable`	特定のクリプトマップ、ダイナミック クリプトマップ、または暗号プロファイルに対するリプレイ検査をディセーブルにします。 （注） このコマンドまたは **set security-association replay window-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

トラブルシューティングのヒント

- 受信されるパケットの数に対して十分高い数字がリプレイ ウィンドウ サイズに設定されていない場合、次のようなシステム メッセージが受信されます。

```
*Nov 17 19:27:32.279: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection
id=1
```

受信されたメッセージが、アンチリプレイ ウィンドウの範囲を超えていると判断されると、上記メッセージが生成されます。

IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定例

アンチ リプレイ ウィンドウのグローバル拡張と無効化：例

次の例は、アンチ リプレイ ウィンドウ サイズがグローバルに 1024 に設定されていることを示しています。

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!
boot-start-marker
```

```
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 192.165.201.2 !
crypto ipsec security-association replay window-size 1024 !
crypto ipsec transform-set basic esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp
 set peer 192.165.201.2
 set transform-set basic
 match address 101
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 192.165.200.2 255.255.255.252  serial restart-delay 0  crypto map mymap !
ip classless
ip route 0.0.0.0 0.0.0.0 192.165.200.1
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101 remark
 Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

暗号マップまたは暗号プロファイルのアンチ リプレイ ウィンドウの拡張および無効化：例

次の例では、アンチ リプレイ検査が、172.17.150.2 への IPsec 接続に関してディセーブルにされているが、172.17.150.3 および 172.17.150.4 への IPsec 接続に関してはイネーブル（および、デフォルトのウィンドウ サイズが 64）にされていることを示しています。

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname networkserver1
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1 enable password ww !
ip subnet-zero
!
cns event-service server
crypto isakmp policy 1
```

```
authentication pre-share
crypto isakmp key cisco170 address 172.17.150.2 crypto isakmp key cisco180 address
172.17.150.3 crypto isakmp key cisco190 address 172.17.150.4
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac crypto ipsec transform-set 180cisco
 esp-des esp-md5-hmac crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
crypto map ETH0 17 ipsec-isakmp
 set peer 172.17.150.2
 set security-association replay disable set transform-set 170cisco match address 170 crypto
 map ETH0 18 ipsec-isakmp  set peer 192.168.1.3 set transform-set 180cisco match address
180 crypto map ETH0 19 ipsec-isakmp set peer 192.168.1.4 set transform-set 190cisco match
address 190 !
interface FastEthernet0
 ip address 172.17.150.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no mop enabled
 crypto map ETH0
!
interface Serial0
 ip address 172.16.160.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
ip classless
ip route 172.18.170.0 255.255.255.0 172.17.150.2 ip route 172.19.180.0 255.255.255.0
172.17.150.3 ip route 172.20.190.0 255.255.255.0 172.17.150.4 no ip http server !
access-list 170 permit ip 172.16.160.0 0.0.0.255 172.18.170.0 0.0.0.255 access-list 180
permit ip 172.16.160.0 0.0.0.255 172.19.180.0 0.0.0.255 access-list 190 permit ip 172.16.160.0
 0.0.0.255 172.20.190.0 0.0.0.255 !
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
logi
end
```

その他の参考資料

次の項では、IPsec アンチ リプレイ ウィンドウの拡張無効化の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Security Command Reference』
IP セキュリティおよび暗号化	IPsec を使用した VPN のセキュリティの設定

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec アンチ リプレイ ウィンドウの拡張と無効化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *1*：*IPsec* アンチ リプレイ ウィンドウの機能情報：拡張と無効化

機能名	リリース	機能情報
IPsec アンチ リプレイ ウィンドウの拡張と無効化	Cisco IOS XE Release 2.1	次のコマンドが導入または変更されました。 **cryptoipsecsecurity-associationreplaydisable**、**ipsecsecurity-associationreplaywindow-size**、**security-associationreplaydisable**、**security-associationreplaywindow-size**.

第 3 章

IPsec VPN の Pre-fragmentation

IPsec VPN の Pre-fragmentation 機能で、最大伝送ユニット（MTU）サイズに近いパケットに対し、暗号化スループットが暗号化ハードウェア アクセラレータの速度で提供されることにより、Cisco IOS XE ルータと VPN クライアントとの間のパフォーマンスが向上します。同じサイズの単位にパケットが分割され、以降の処理ではフラグメンテーションが不要になります。

- 機能情報の確認，13 ページ
- IPsec VPN の Pre-fragmentation の制約事項，13 ページ
- IPsec VPN の Pre-fragmentation に関する情報，15 ページ
- IPsec VPN の Pre-fragmentation の設定方法，16 ページ
- その他の参考資料，17 ページ
- IPsec VPN の Pre-fragmentation の機能情報，18 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPsec VPN の Pre-fragmentation の制約事項

この機能の設定前に次の情報を考慮してください。

- IPsec VPN の Pre-fragmentation は IPsec トンネル モードおよび GRE を使用する IPsec トンネル モードで動作し、IPsec トランスポート モードでは動作しません。
- トラフィックが単一方向のネットワーク上で復号ルータに IPsec VPN の Pre-fragmentation を設定しても、パフォーマンスは向上せず、それぞれのピアの動作は変わりません。
- 発信パケットの圧縮がオンになっている場合は、IPsec VPN の Pre-fragmentation は変換前に実行されます。
- IPsec VPN の Pre-fragmentation は、出力インターフェイス **cryptoipsecdf-bit** の設定と着信パケットの「do not fragment」（DF）ビットの状態によって機能が異なります。次の表を参照してください。

表 *2*：***IPsec VPN の Pre-fragmentation の依存関係***

IPsec VPN の Pre-fragmentation 機能の状態（イネーブル/ディセーブル）	**出力インターフェイス「crypto ipsec df-bit」の設定**	**着信パケット DF ビットの状態**	**結果**
イネーブル	crypto ipsec df-bit クリア	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit クリア	1	暗号化前にフラグメンテーションが実行されます。
ディセーブル	crypto ipsec df-bit クリア	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit クリア	1	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
イネーブル	crypto ipsec df-bit セット	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit セット	1	パケットがドロップされます。

IPsec VPN の Pre-fragmentation 機能の状態（イネーブル/ディセーブル）	出力インターフェイス「crypto ipsec df-bit」の設定	着信パケット DF ビットの状態	結果
ディセーブル	crypto ipsec df-bit セット	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit セット	1	パケットがドロップされます。
イネーブル	crypto ipsec df-bit コピー	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit コピー	1	パケットがドロップされます。
ディセーブル	crypto ipsec df-bit コピー	0	暗号化の後にフラグメンテーションが発生し、復号化の前にパケットがリアセンブルされます。
ディセーブル	crypto ipsec df-bit コピー	1	パケットがドロップされます。

IPsec VPN の Pre-fragmentation に関する情報

IPsec VPN の Pre-fragmentation

パケットのサイズが暗号化ルータのアウトバウンド リンクの MTU のサイズに近く、IPsec ヘッダー付きでカプセル化されている場合は、アウトバウンド リンクの MTU を超えることがあります。これにより、暗号化後にパケット フラグメンテーションが発生します。よって復号化ルータでは、その復号化ルータのパフォーマンスを低下させているプロセス パスの当該パケットがリアセンブルされる必要があります。

IPsec VPN の Pre-fragmentation 機能により、プロセス パスではなく高パフォーマンスの CEF パスで復号化ルータが動作可能になるため、その復号化ルータのパフォーマンスが向上します。復号化ルータでは、トランスフォーム セット（IPsec セキュリティ アソシエーション（SA）の一部と

して設定）の利用可能な情報を基に、カプセル化されているパケットのサイズを事前に確認できます。パケットのサイズが出力インターフェイスのMTUを超えることが前もって確認されると、パケットは暗号化前にフラグメント化（分割）されます。この機能を使用すると、復号化前にプロセス レベルでパケットをリアセンブルすることがなくなるため、復号化のパフォーマンスとIPsec トラフィックの全体的なスループットが向上します。

（注） トンネル インターフェイスの Pre-fragmentation 機能はデフォルトでオフになっています。Pre-fragmentation によってパフォーマンスを向上させるには、トンネル インターフェイスの両端に同じ MTU があるようにしてから、Pre-fragmentation をオンにします。

暗号マップは、暗号化の前後に発生するフラグメンテーションの動作を定義するためには使用されなくなっています。現在、IPsec 仮想トンネル インターフェイス（仮想テンプレート インターフェイスともいう）（VTI）のフラグメンテーションの動作は、VTI で設定されている IP MTU の設定によって決定されます。

VTI の詳細については、IPsec 仮想トンネル インターフェイス機能のドキュメントを参照してください。

（注） フラグメンテーションを暗号化後に動作させる場合、VTI の IP MTU は、出力ルータ インターフェイスの IP MTU よりも大きい値に設定します。IP MTU の値を表示するには、**showipinterfacetunnel** コマンドを使用します。

IPsec VPN の Pre-fragmentation の設定方法

IPsec VPN の Pre-fragmentation の設定

このタスクを実行して、IPsec VPN の Pre-Fragmentation を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipmtu***bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Router(config-if)# interface tunnel0`	VTI が設定されるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipmtu***bytes* 例： `Router(config-if)# ip mtu 1500` 例：	IPsec VPN の出力インターフェイスにおける IP パケットの VTI MTU サイズをバイト単位で設定します。 （注） フラグメンテーションを暗号化後に動作させる場合、VTI の IP MTU は、出力ルータ インターフェイスの IP MTU よりも大きい値に設定します。IP MTU の値を表示するには、**show ip interface tunnel** コマンドを使用します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS XE コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	『Cisco IOS Security Command Reference』
IPSec	IPsec 仮想トンネル インターフェイス機能のドキュメント

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

IPsec VPN の Pre-fragmentation の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *3*：*IPsec VPN の Pre-fragmentation* の機能情報

機能名	リリース	機能情報
IPsec VPN の Pre-fragmentation	Cisco IOS XE 2.1	この機能で、最大伝送ユニット（MTU）サイズに近いパケットに対し、暗号化スループットが暗号化ハードウェア アクセラレータの速度で提供されることにより、Cisco IOS XE ルータと VPN クライアントとの間のパフォーマンスが向上します。同じサイズの単位にパケットが分割され、以降の処理ではフラグメンテーションが不要になります。 次のコマンドが導入または変更されました。**ipmtu（インターフェイス コンフィギュレーション）.**

第 4 章

Invalid Security Parameter Index Recovery

IP セキュリティ（IPsec）パケットの処理中に無効なセキュリティ パラメータ インデックス エラー（「Invalid SPI」として表示されます）が発生した場合、Invalid Security Parameter Index Recovery 機能によって、インターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（SA）を確立できます。「IKE」モジュールによって「Invalid SPI」エラーの通知が、発信側の IPsec ピアに対して送信され、セキュリティ アソシエーション データベース（SADB）の再同期化と、成功したパケット処理の再開が可能になります。

- 機能情報の確認，21 ページ
- Invalid Security Parameter Index Recovery の前提条件，22 ページ
- Invalid Security Parameter Index Recovery の制約事項，22 ページ
- Invalid Security Parameter Index Recovery に関する情報，22 ページ
- Invalid Security Parameter Index Recovery の設定方法，23 ページ
- Invalid Security Parameter Index Recovery の設定例，29 ページ
- その他の参考資料，34 ページ
- Invalid Security Parameter Index Recovery の機能情報，35 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

Invalid Security Parameter Index Recovery の前提条件

Invalid Security Parameter Index Recovery 機能を設定する前に、ルータ上で IKE および IPsec を有効化しておく必要があります。

Invalid Security Parameter Index Recovery の制約事項

IPsec ピアに対して「Invalid SPI」エラーを通知するために IKE SA を開始する場合、サービス妨害（DoS）攻撃が発生するリスクがあります。Invalid Security Parameter Index Recovery 機能には、そのようなリスクを最小化するためのメカニズムが内蔵されていますが、リスクが存在するため、Invalid Security Parameter Index Recovery 機能は、デフォルトでは有効化されていません。コマンド ライン インターフェイス（CLI）を使用してコマンドをイネーブルにする必要があります。

Invalid Security Parameter Index Recovery に関する情報

機能の動作

ある IPsec ピアが「死ぬ」（たとえば、リブートが発生したり、IPsec ピアが何らかの理由によりリセットされたりした場合にピアが「死ぬ」可能性があります）と、IPsec の「ブラック ホール化」が発生します。ピアの 1 つ（受信側のピア）は完全にリセットされるため、そのピアでは他のピアとの IKE SA が失われます。一般に、IPsec ピアによって、SA を検出できないパケットが受信されると、そのピアによって、そのデータの発信者に対する IKE「INVALID SPI NOTIFY」メッセージの送信が試行されます。この通知は IKE SA を使用して送信されます。IKE SA が使用できない場合、受信側のピアによってパケットが廃棄されます。

（注） 1 つの SA につきピアは 2 つだけです。しかし、SADB は複数の SA を持てます。これにより、各 SA は異なるピアとのアソシエーションを持ちます。

無効なセキュリティ パラメータ インデックス（SPI）が発生した場合、Invalid Security Parameter Index 機能によって、データの発信者に IKE SA が設定され、IKE「INVALID SPI NOTIFY」メッセージが送信されます。データを発信したピアによって「INVALID SPI NOTIFY」メッセージが「参照」され、無効な SPI を持つ IPsec SA が削除されます。発信側のピアからトラフィックがさらにある場合、IPsec SA は存在せず、新しい SA が設定されます。トラフィックが再び流れます。デフォルトの動作（つまり、Invalid Security Parameter Index 機能が設定されていない状態）では、無効な SPI エラーの原因となったデータ パケットは廃棄されます。発信側のピアによって、無効な SPI を持つ IPsec SA を使用したデータの送信が続けられ、受信側のピアによってトラフィックが廃棄され続けます（その結果、「ブラック ホール」が作成されます）。

IPsec モジュールでは IKE モジュールが使用され、他のピアに IKE「INVALID SPI NOTIFY」メッセージが送信されます。無効な SPI リカバリが行われると、IPsec SA の設定自体によっていくつかのパケットが廃棄されますが、意味のあるパケット廃棄は一切行われません。

Invalid Security Parameter Index Recovery 機能用にルータを設定するには、**crypto isakmp invalid-spi-recovery** コマンドを使用します。IKE SA は、このコマンドを設定しない限り開始されません。

Invalid Security Parameter Index Recovery の設定方法

Invalid Security Parameter Index Recovery の設定

Invalid Security Parameter Index Recovery 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpinvalid-spi-recovery**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmpinvalid-spi-recovery** 例： `Router (config)#` **crypto isakmp invalid-spi-recovery**	IKE モジュール プロセスを開始します。それにより、IKE モジュールによって、受信側ピアに対して「Invalid SPI」エラーが発生したことが通知されます。

事前共有設定の確認

2 つのピア間におけるトラフィックに関する IPsec SA のステータスを確認するには、**showcryptoipsecsa** コマンドを使用します。IPsec SA が、あるピアでは使用可能で、他のピアでは使用不可の場合、「ブラック ホール化」の状況が発生します。この場合、無効な SPI エラーが受信側のピアのログに記録されます。コンソールロギングをオンにするか、シスログサーバを確認すると、これらのエラーもログに記録されていることがわかります。

次の図に、一般的な事前共有設定のトポロジを示します。ホスト 1 が発信側のピア（発信側）、ホスト 2 が受信側のピア（応答側）です。

図 *1*：事前共有設定トポロジ

手順の概要

1. ホスト 1 とホスト 2 の間における IKE および IPsec SA を開始します。
2. ルータ B 上の IKE および IPsec SA をクリアします。
3. ホスト 1 からのトラフィックをホスト 2 に送信し、新しい IKE および IPsec SA が正しく確立されているかどうかを確認します。
4. ルータ B に無効な SPI メッセージがないか確認します。

手順の詳細

ステップ 1 ホスト 1 とホスト 2 の間における IKE および IPsec SA を開始します。

ルータ A

例：

```
Router# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       / 10.2.2.2              10.1.1.1        QM_IDLE               1       0
```

ルータ B

例：

```
Router# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.1.1.1       10.2.2.2        QM_IDLE               1       0
```

ルータ A

例：

```
Router# show crypto ipsec sa interface fastethernet0/0
interface: FastEthernet0/0
    Crypto map tag: testtag1, local addr. 10.1.1.1
   protected vrf:
```

```
   local  ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   current_peer: 10.2.2.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.2
     path mtu 1500, media mtu 1500
     current outbound spi: 7AA69CB7
     inbound esp sas:
      spi: 0x249C5062(614223970)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537831/3595)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
      spi: 0xB16D1587(2976716167)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537831/3595)
        replay detection support: Y
     inbound pcp sas:
     outbound esp sas:
      spi: 0x7AA69CB7(2057739447)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537835/3595)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
      spi: 0x1214F0D(18960141)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537835/3594)
        replay detection support: Y
     outbound pcp sas:
```

ルータ B

例：

```
Router# show crypto ipsec sa interface Fastethernet1/0
interface: FastEthernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
```

```
    path mtu 1500, media mtu 1500
    current outbound spi: 249C5062
    inbound esp sas:
     spi: 0x7AA69CB7(2057739447)
       transform: esp-des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
       crypto engine type: Hardware
       sa timing: remaining key lifetime (k/sec): (4421281/3593)
       IV size: 8 bytes
       replay detection support: Y
    inbound ah sas:
     spi: 0x1214F0D(18960141)
       transform: ah-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
       crypto engine type: Hardware
       sa timing: remaining key lifetime (k/sec): (4421281/3593)
       replay detection support: Y
    inbound pcp sas:
    outbound esp sas:
     spi: 0x249C5062(614223970)
       transform: esp-des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
       crypto engine type: Hardware
       sa timing: remaining key lifetime (k/sec): (4421285/3593)
       IV size: 8 bytes
       replay detection support: Y
    outbound ah sas:
     spi: 0xB16D1587(2976716167)
       transform: ah-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
       crypto engine type: Hardware
       sa timing: remaining key lifetime (k/sec): (4421285/3592)
       replay detection support: Y
    outbound pcp sas:
```

ステップ 2 ルータ B 上の IKE および IPsec SA をクリアします。

例：

```
Router# clear crypto isakmp
Router# clear crypto sa
Router# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
      /        10.2.2.2.       10.1.1.1      MM_NO_STATE           1       0 (deleted)
Router# show crypto ipsec sa
interface: FastEthernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 0
     inbound esp sas:
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
```

```
     outbound ah sas:
     outbound pcp sas:
```

ステップ 3 ホスト 1 からのトラフィックをホスト 2 に送信し、新しい IKE および IPsec SA が正しく確立されているかどうかを確認します。

例：

```
ping
Protocol [ip]: ip
Target IP address: 10.0.2.2
Repeat count [5]: 30
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]: no
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (28/30), round-trip min/avg/max = 1/3/8 ms
RouterB# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.1.1.1       10.2.2.2     QM_IDLE              3       0
       /        10.1.1.1       10.2.2.2      MM_NO_STATE           1       0 (deleted)
RouterB# show crypto ipsec sa
interface: FastEthernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: D763771F
     inbound esp sas:
      spi: 0xE7AB4256(3886760534)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5127, flow_id: 3, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502463/3596)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
      spi: 0xF9205CED(4179647725)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5125, flow_id: 3, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502463/3596)
        replay detection support: Y
     inbound pcp sas:
     outbound esp sas:
      spi: 0xD763771F(3613619999)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5128, flow_id: 4, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502468/3596)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
```

```
      spi: 0xEB95406F(3952427119)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5126, flow_id: 4, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502468/3595)
        replay detection support: Y
     outbound pcp sas:
RouterA# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.2.2.2       10.1.1.1      MM_NO_STATE           1       0 (deleted)
       /        10.2.2.2       10.1.1.1      QM_IDLE               2       0
```

ステップ 4 ルータ B に無効な SPI メッセージがないか確認します。

例：

```
Router# show logging
Syslog logging: enabled (10 messages dropped, 13 messages rate-limited, 0 flushes, 0 overruns, xml
 disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 43 messages logged, xml disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged
Log Buffer (8000 bytes):
*Mar 24 20:55:45.739: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for

        destaddr=10.2.2.2, prot=51, spi=0x1214F0D(18960141), srcaddr=10.1.1.1
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #2,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:47.743: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar 24 20:55:47.743: IPSEC(spi_response): getting spi 4179647725 for SA
        from 10.2.2.2        to 10.1.1.1     for prot 2
*Mar 24 20:55:47.747: IPSEC(spi_response): getting spi 3886760534 for SA
        from 10.2.2.2     to 10.1.1.1        for prot 3
*Mar 24 20:55:48.071: IPSec: Flow_switching Allocated flow for flow_id 939524099
*Mar 24 20:55:48.071: IPSec: Flow_switching Allocated flow for flow_id 939524100
*Mar 24 20:55:48.135: IPSEC(key_engine): got a queue event with 4 kei messages
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xF9205CED(4179647725), conn_id= 939529221, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xEB95406F(3952427119), conn_id= 939529222, keysize= 0, flags= 0xA
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
```

```
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xE7AB4256(3886760534), conn_id= 939529223, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xD763771F(3613619999), conn_id= 939529224, keysize= 0, flags= 0xA
*Mar 24 20:55:48.139: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:48.139: IPSEC(mtree_add_ident): src 10.2.2.2, dest 10.1.1.1, dest_port 0
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 51,
    sa_spi= 0xF9205CED(4179647725),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529221
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.2.2.2, sa_prot= 51,
    sa_spi= 0xEB95406F(3952427119),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529222
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0xE7AB4256(3886760534),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529223
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.2.2.2, sa_prot= 50,
    sa_spi= 0xD763771F(3613619999),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529224
ipseca-72a#
```

Invalid Security Parameter Index Recovery の設定例

Invalid Security Parameter Index Recovery：例

次に、Invalid Security Parameter Index Recovery がルータ A とルータ B に設定されている例を示します。Invalid Security Parameter Index Recovery：例, （29 ページ）には、この例で使用されるトポロジを示します。

ルータ A

```
Router# show running-config
Building configuration...
Current configuration : 2048 bytes
!
version 2.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service tcp-small-servers
!
hostname ipseca-71a
!
logging queue-limit 100
no logging console
```

```
enable secret 5 $1$4GZB$L2YOmnenOCNAu0jgFxebT/
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.2.2.2
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.2.2.2
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.0.0.0
 no ip route-cache cef
 duplex full
 speed 100
 crypto map testtag1
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 no ip route-cache cef
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
```

```
 serial restart_delay 0
!
interface Serial1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.3.3.3 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.0.1 host 10.0.2.2
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
 login
!
!
end
ipseca-71a#
```

ルータ B

```
Router# show running-config
Building configuration...
Current configuration : 2849 bytes
!
version 2.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ipseca-72a
!
logging queue-limit 100
no logging console
enable secret 5 $1$kKqL$5Th5Qhw1ubDkkK90KWFxi1
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
```

```
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.1.1.1
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 10.2.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
 crypto map testtag1
!
interface FastEthernet1/1
 ip address 10.0.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
!
interface FastEthernet1/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/4
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/5
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
```

```
!
interface FastEthernet1/6
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/7
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial3/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.2.2 host 10.0.0.1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
```

```
 stopbits 1
line vty 0 4
 password lab
 login
!
!
end
```

その他の参考資料

次の項では、Invalid Security Parameter Index Recovery に関連した参考資料を示します。

関連資料

関連項目	マニュアル タイトル
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
インターフェイス コマンド	『Cisco IOS Master Command List』

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Invalid Security Parameter Index Recovery の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *4*：*Invalid Security Parameter Index Recovery* の機能情報

機能名	リリース	機能情報
Invalid Special Parameter Index（SPI）Recovery	Cisco IOS XE Release 2.1	IPsec パケット処理で、無効な SPI が検出された場合は、Invalid Security Parameter Index Recovery 機能によって、IKE SA が確立されます。「IKE」モジュールによって「Invalid SPI」エラーの通知が、発信側の IPsec ピアに対して送信され、セキュリティ アソシエーションデータベース（SADB）の再同期化と、成功したパケット処理の再開が可能になります。 次のコマンドが導入または変更されました。 **cryptoisakmpinvalid-spi-recovery.**

第 5 章

IPSec デッド ピア検出定期メッセージ オプション

IPSec デッド ピア検出定期メッセージ オプション機能を使用すれば、ルータに対し、そのインターネット キーエクスチェンジ（IKE）ピアの活性を定期的に照会するよう設定できます。このオプションを使用すると、デフォルトのオンデマンド デッド ピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。

- 機能情報の確認，37 ページ
- IPSec デッド ピア検出定期メッセージ オプションの前提条件，38 ページ
- IPSec デッド ピア検出定期メッセージ オプションの制約事項，38 ページ
- IPSec デッド ピア検出定期メッセージ オプションに関する情報，38 ページ
- IPSec デッド ピア検出定期メッセージ オプションの設定方法，40 ページ
- IPSec デッド ピア検出定期メッセージ オプションの設定例，45 ページ
- その他の参考資料，49 ページ
- デッド ピア検出定期メッセージ オプションの機能情報，51 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPSec デッド ピア検出定期メッセージ オプションの前提条件

IPSec デッド ピア検出定期メッセージ オプション機能を設定するには、次のことが必要です。

- IP セキュリティ（IPsec）の設定についての知識。
- DPD（Dead Peer Detection）がサポートされている IKE ピア。DPD をサポートしているのは、Cisco VPN 3000 コンセントレータ、Cisco PIX ファイアウォール、Cisco VPN Client、およびすべての動作モードの Cisco IOS XE ソフトウェア（サイト間、Easy VPN リモート、Easy VPN サーバ）などです。

IPSec デッド ピア検出定期メッセージ オプションの制約事項

定期的な DPD を使用すると、ルータによって、オンデマンドの DPD と比較してより速い応答時間で無応答の IKE ピアを検知できる可能性があります。ただし、定期的な DPD では、余分なオーバーヘッドが発生します。大量の IKE ピアと通信する場合は、オンデマンドの DPD の方を検討してください。

IPSec デッド ピア検出定期メッセージ オプションに関する情報

DPD および Cisco IOS XE キープアライブ機能の動作

DPD および Cisco IOS XE キープアライブは、タイマーに基づいて機能します。タイマーが 10 秒に設定されている場合、ルータは 10 秒毎に「hello」メッセージが送信されます（もちろん、ルータによってピアからの「hello」メッセージが受信された場合は除きます）。IOS キープアライブおよび定期的な DPD の利点は、デッド ピアの検知が早くなることです。しかし、IOS キープアライブおよび定期的な DPD では、かなりの頻度でメッセージを定期的に送信する必要があります。頻繁にメッセージを送信する結果、通信を行うピアによって暗号化および復号化しなければならないパケット数が増加します。

DPD にはオンデマンド方式もあります。対称的なこのオンデマンド方式がデフォルトです。オンデマンド DPD では、トラフィック パターンに基づいてメッセージが送信されます。たとえば、ルータによって発信トラフィックが送信される必要があり、ピアの活性に疑問がある場合、ルータによって DPD メッセージが送信され、ピアのステータスが照会されます。ルータに送信するトラフィックがない場合、DPD メッセージは送信されません。ピアが停止しており、ピアに送信す

るトラフィックがルータにない場合、IKE または IPsec セキュリティ アソシエーション（SA）のキー再生成が必要でないかぎり、ルータによる検知は行われません（ルータによるピアとの通信が行われない場合、ピアの活性は重要ではありません）。一方、ピアに送信するトラフィックがルータにあり、ピアの応答がない場合は、ピアのステートを判断するために、ルータによって DPD メッセージが開始されます。

IPSec デッド ピア検出定期メッセージ オプションの使用

IPSec デッド ピア検出（DPD）定期メッセージ オプション機能では、DPD メッセージが定期的に「強制される」ようルータを設定できます。この強制方式の結果、デッド ピアが早期に検知されます。たとえば、送信するトラフィックがルータにない場合でも、DPD メッセージが定期的に送信され、ピアが停止していた場合、IKE SA による検知がタイムアウトになるまでルータが待機する必要はありません。

DPD 定期メッセージ オプションを設定する場合、**cryptoisakmpkeepalive** コマンドは **periodic** キーワードを指定して使用する必要があります。**periodic** キーワードを指定しない場合、ルータはデフォルトのオンデマンド方式になります。

（注） **cryptoisakmpkeepalive** コマンドを設定すると、Cisco IOS ソフトウェアは、ピアがサポートしているプロトコルに応じて、Cisco IOS キープアライブまたは DPD の使用についてネゴシエーションを行います。

暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブ機能の使用

暗号マップ内で DPD および Cisco IOS XE キープアライブ機能を複数のピアと組み合わせることにより、ステートレス フェールオーバーを実現できます。DPD により、ルータによる停止 IKE ピアの検知が可能となり、ルータによって停止状態が検知されると、ルータによってピアに対する IPsec と IKE SA が削除されます。複数のピアを設定している場合、ルータによって、次にリストされているピアへの切り替えが行われ、ステートレス フェールオーバーが実現します。

Easy VPN Remote コンフィギュレーション内での DPD の使用

Easy VPN Remote コンフィギュレーション内で DPD を使用できます。セクション「Easy VPN Remote の DPD の設定」を参照してください。

IPSec デッド ピア検出定期メッセージ オプションの設定方法

定期的な DPD メッセージの設定

定期的な DPD メッセージを設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpkeepalive***seconds* [*retries*] [**periodic** | **on-demand**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmpkeepalive***seconds* [*retries*] [**periodic** | **on-demand**] 例： `Router (config)# crypto isakmp keepalive 10 periodic`	ゲートウェイによるピアへの DPD メッセージの送信を許可します。 • *seconds*：**periodic** キーワードを使用する場合、この引数には DPD メッセージの間隔を秒数で指定します。範囲は 10 ～ 3600 秒です。 **on-demand** キーワードを使用する場合、この引数には、送信するデータ（IPSec）トラフィックがあるときに、DPD リトライ メッセージを送信するまでピアからトラフィックを受信しない間に待機する秒数を指定します。範囲は 10 ～ 3600 秒です。 （注） 間隔を指定しない場合、エラー メッセージが表示されます。 • *retry-seconds*：（任意）ピアによって DPD リトライ メッセージが失われた場合の DPD リトライ メッセージの送信間隔を秒数で指定します。範囲は 2 ～ 60 秒です。

	コマンドまたはアクション	目的
		1 つの DPD メッセージがピアで失われると、ルータはよりアグレッシブな状態に移行し、より短いリトライ間隔で DPD リトライ メッセージを送信します。ピアによって DPD リトライ メッセージが失われた場合のこの間隔は、DPD リトライ間の秒数です。デフォルトで、DPD リトライ メッセージは 2 秒ごとに送信されます。アグレッシブな 5 回の DPD リトライ メッセージが失われると、トンネルがダウンした状態としてマークされます。 （注） IPsec ハイ アベイラビリティ（HA）を使用して DPD を設定するには、デフォルト（2 秒）以外の値を使用することを推奨します。HA には、キープアライブ時間を 10 秒、試行を 5 回に設定するのが適しています。その時間が、ルータがアクティブ モードになるためにかかる時間であるからです。 • **periodic**：（任意）DPD メッセージが定期的に送信されます。 • **on-demand**：（任意）デフォルトの動作です。DPD リトライがオンデマンドで送信されます。 （注） このオプションはデフォルトであるため、**on-demand** キーワードは設定の出力に表示されません。

暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブの設定

DPD および IOS キープアライブを、クリプト マップと組み合わせて使用するように設定し、ステートレス フェールオーバーを実現するには、次の手順を実行します。この設定により、最初のピアが停止していることが検知されると、ルータによってピア リストが循環されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptomap***map-nameseq-num***ipsec-isakmp**
4. **setpeer** {*host-name* [**dynamic**] | *ip-address*}
5. **settransform-set***transform-set-name*
6. **matchaddress** [*access-list-id* | *name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptomap***map-nameseq-num***ipsec-isakmp** 例： `Router (config)# crypto map green 1 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。 • **ipsec-isakmp** キーワードは、この暗号マップ エントリによって指定されたトラフィックを保護するための IPsec SA を確立するために、IKE が使用されることを示します。
ステップ 4	**setpeer** {*host-name* [**dynamic**] | *ip-address*} 例： `Router (config-crypto-map)# set peer 10.12.12.12`	クリプト マップ内の IPsec ピアを指定します。 • このコマンドを繰り返すことによって、複数のピアを指定できます。
ステップ 5	**settransform-set***transform-set-name* 例： `Router (config-crypto-map)# set transform-set txfm`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。 • このコマンドを繰り返すことによって、複数のトランスフォーム セットを指定できます。
ステップ 6	**matchaddress** [*access-list-id* | *name*] 例： `Router (config-crypto-map)# match address 101`	クリプト マップ エントリの拡張アクセス リストを指定します。

Easy VPN Remote の DPD の設定

Easy VPN Remote コンフィギュレーション内で DPD を設定するには、次の手順を実行します。この設定によっても、最初のピアが停止していることが検知されると、ルータによってピア リストが循環されます。

（注） Cisco IOS XE キープアライブは、Easy VPN Remote コンフィギュレーションではサポートされていません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoipsecclientezvpn***name*
4. **connect** {**auto** | **manual**}
5. **group***group-name***key***group-key*
6. **mode** {**client** | **network-extension**}
7. **peer** {*ipaddress* | *hostname*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoipsecclientezvpn***name* 例： `Router (config)# crypto ipsec client ezvpn ezvpn-config1`	Cisco Easy VPN Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**connect** {**auto** | **manual**} 例： `Router (config-crypto-ezvpn)# connect manual`	要求に応じて、IPsec VPN トンネルを手動で確立および終了します。 • **auto** キーワードオプションはデフォルト設定です。
ステップ 5	**group***group-name* **key***group-key* 例： `Router (config-crypto-ezvpn)# group unity key preshared`	バーチャルプライベートネットワーク（VPN）接続用のグループ名およびキー値を指定します。
ステップ 6	**mode** {**client** | **network-extension**} 例： `Router (config-crypto-ezvpn)# mode client`	ルータの動作の VPN モードを指定します。
ステップ 7	**peer** {*ipaddress* | *hostname*} 例： `Router (config-crypto-ezvpn)# peer 10.10.10.10`	VPN 接続に対して、ピアの IP アドレスまたはホスト名を設定します。 • ホスト名を指定できるのは、ルータから DNS サーバを介してホスト名解決を行える場合に限りにます。 • このコマンドは複数回繰り返して実行できます。

DPD が有効化されていることの確認

DPD を使用すれば、ピアが到達不能になった時に、ルータによる IKE ステートのクリアが可能になります。DPD が有効化されており、ピアがしばらくの間到達不能になった場合、**clear crypto session** コマンドを使用して、手動で IKE と IPsec SA をクリアできます。

debug crypto isakmp コマンドを使用すると、DPD が有効化されていることを確認できます。

手順の概要

1. イネーブル化
2. **clearcryptosession** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*]
3. **debugcryptoisakmp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearcryptosession** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*] 例： `Router# clear crypto session`	暗号セッション（IPsec および IKE SA）を削除します。
ステップ 3	**debugcryptoisakmp** 例： `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。

IPSec デッド ピア検出定期メッセージ オプションの設定例

定期的な DPD を有効化したサイト間設定の例

次の設定は、定期的な DPD をイネーブルにしていないサイト間設定用です。設定は、IKE フェーズ 1 ポリシー用と IKE 事前共有キー用です。

IKE フェーズ 1 ポリシー

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
!
```

IKE 事前共有キー

```
crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac
```

```
!
!
interface
  ip address 10.1.32.14 255.255.255.0
  speed auto

!
```

DPD を有効化した Easy VPN Remote の例

次の設定は、ルータに対して、30 秒毎に定期的な DPD メッセージを送信するように指示するものです。ピアによる DPD R_U_THERE メッセージに対する応答が失敗した場合、ルータによって、20 秒毎にメッセージが再送信されます（全部で 4 回の転送）。

```
crypto isakmp keepalive 30 20 periodic
crypto ipsec client ezvpn ezvpn-config
  connect auto
  group unity key preshared
  mode client
  peer 10.2.80.209
!
!
interface FastEthernet0
  ip address 10.2.3.4 255.255.255.0
  half-duplex
  crypto ipsec client ezvpn ezvpn-config inside
!
interface FastEthernet0
  ip address 10.1.32.14 255.255.255.0
  speed auto
  crypto ipsec client ezvpn ezvpn-config outside
```

debug crypto isakmp コマンドを使用した DPD 設定の確認の例

次の **debug crypto isakmp** コマンドの出力例では、IKE DPD が有効化されていることを確認しています。

```
*Mar 25 15:17:14.131: ISAKMP:(0:1:HW:2):IKE_DPD is enabled, initializing timers
```

IKE DPD がイネーブルになっていること（および、ピアによって DPD がサポートされていること）を確認するには、定期的なDPDをイネーブルにする時に、コマンドによって指定された間隔で次のデバッグ メッセージが出力されることを確認する必要があります。

```
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2):purging node 899852982 *Mar 25 15:18:52.111:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:18:52.111: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

上記のメッセージは、DPD R_U_THERE メッセージの送信に対応しています。

```
*Mar 25 15:18:52.123: ISAKMP (0:268435457): received packet from 10.2.80.209
dport 500 sport 500 Global (I) QM_IDLE
*Mar 25 15:18:52.123: ISAKMP: set new node -443923643 to QM_IDLE *Mar 25 15:18:52.131:
ISAKMP:(0:1:HW:2): processing HASH payload. message ID =
-443923643
*Mar 25 15:18:52.131: ISAKMP:(0:1:HW:2): processing NOTIFY R_U_THERE_ACK protocol 1
```

```
 spi 0, message ID = -443923643, sa = 81BA4DD4
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2): DPD/R_U_THERE_ACK received from peer
10.2.80.209, sequence 0x9
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):deleting node -443923643 error FALSE
reason "informational (in) state 1"
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY *Mar
25 15:18:52.135: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

上記のメッセージは、ピアからの確認応答（ACK）メッセージに対応しています。

```
Router#
*Mar 25 15:47:35.335: ISAKMP: set new node -90798077 to QM_IDLE *Mar 25 15:47:35.343:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:35.343: ISAKMP:(0:1:HW:2):purging node -90798077 *Mar 25 15:47:35.347:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:47:35.347: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:36.611: ISAKMP:(0:1:HW:2):purging node 1515050537 *Mar 25 15:47:37.343:
ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:37.343: ISAKMP: set new node -1592471565 to QM_IDLE *Mar 25 15:47:37.351:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:37.351: ISAKMP:(0:1:HW:2):purging node -1592471565 *Mar 25 15:47:37.355:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:37.355: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:39.355: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:39.355: ISAKMP: set new node 1758739401 to QM_IDLE *Mar 25 15:47:39.363:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:39.363: ISAKMP:(0:1:HW:2):purging node 1758739401 *Mar 25 15:47:39.367:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:39.367: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:41.367: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:41.367: ISAKMP: set new node 320258858 to QM_IDLE *Mar 25 15:47:41.375:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):purging node 320258858 *Mar 25 15:47:41.379:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:43.379: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:43.379: ISAKMP: set new node -744493014 to QM_IDLE *Mar 25 15:47:43.387:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:43.387: ISAKMP:(0:1:HW:2):purging node -744493014 *Mar 25 15:47:43.391:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:43.391: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):peer 10.2.80.209 not responding! *Mar 25 15:47:45.391:
 ISAKMP:(0:1:HW:2):peer does not do paranoid keepalives.
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE       (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.395: ISAKMP: Unlocking IPSEC struct 0x81E5C4E8 from
delete_siblings, count 0
*Mar 25 15:47:45.395: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
10.2.80.209:500       Id: 10.2.80.209
*Mar 25 15:47:45.399: ISAKMP: set new node -2061951065 to QM_IDLE *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
```

```
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):purging node -2061951065 *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_DEST_SA
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE       (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.415: ISAKMP: Unlocking IKE struct 0x81E5C4E8 for
isadb_mark_sa_deleted(), count 0
*Mar 25 15:47:45.415: ISAKMP: Deleting peer node by peer_reap for 10.2.80.209:
81E5C4E8
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -1067612752 error TRUE
reason "peers alive"
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -114443536 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node 2116015069 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node -1981865558 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL *Mar 25
15:47:45.419: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA  New State =
IKE_DEST_SA
*Mar 25 15:47:45.419: ISAKMP: received ke message (4/1)
*Mar 25 15:47:45.419: ISAKMP: received ke message (3/1)
*Mar 25 15:47:45.423: ISAKMP: ignoring request to send delete notify (no ISAKMP
sa) src 10.1.32.14 dst 10.2.80.209 for SPI 0x3A7B69BF
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting SA reason "" state (I)
MM_NO_STATE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -1067612752 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -114443536 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node 2116015069 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):deleting node -1981865558 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH *Mar 25
15:47:45.427: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA  New State =
IKE_DEST_SA
```

上記のメッセージは、リモート ピアが到達不能なっている時に何が発生しているのかを示しています。ルータによって、最終的に IPsec および SA が削除される前に、1 つの DPD R_U_THERE メッセージおよび 4 つの転送が送信されます。

暗号マップ内の複数のピアとの組み合わせで使用される DPD および Cisco IOS XE キープアライブ：例

次に、セキュリティ アソシエーション（SA）を確立するために IKE が使用される場合に、DPD および Cisco IOS XE キープアライブが暗号マップ設定内の複数のピアとの組み合わせで使用される例を示します。この例では、SA が、10.0.0.1、10.0.0.2、または 10.0.0.3 の IPsec ピアに設定される可能性があります。

```
crypto map green 1 ipsec-isakmp
  set peer 10.0.0.1
  set peer 10.0.0.2
  set peer 10.0.0.3
  set transform-set txfm
  match address 101
```

Easy VPN Remote の複数のピアとの組み合わせで使用される DPD の例

次に、DPD が Easy VPN Remote コンフィギュレーション内の複数のピアとの組み合わせで使用される例を示します。この例では、SA が、10.10.10.10、10.2.2.2、または 10.3.3.3 の IPsec ピアに設定される可能性があります。

```
crypto ipsec client ezvpn ezvpn-config
  connect auto
  group unity key preshared
  mode client
  peer 10.10.10.10
  peer 10.2.2.2
  peer 10.3.3.3
```

その他の参考資料

次の項では、IPSec デッド ピア検出定期メッセージ オプションの関連資料を示します。

関連資料

関連項目	マニュアル タイトル
IPsec の設定	IPsec を使用した VPN のセキュリティの設定
IPsec コマンド	『Cisco IOS Security Command Reference』

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
DPD は、インターネット ドラフト「draft-ietf-ipsec-dpd-04.txt」に準拠しています。このドラフトは、Informational RFC（番号はまだ割り当てられていません）として公表の検討中です。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

デッド ピア検出定期メッセージ オプションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *5*：デッド ピア検出の機能情報

機能名	リリース	機能情報
デッド ピア検出定期メッセージ オプション	Cisco IOS XE Release 2.1	この機能により、ルータに対し、その IKE ピアの有効性について定期的に照会が行われるよう設定できます。このオプションを使用すると、デフォルトのオンデマンド デッド ピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。 次のコマンドが導入または変更されました。 **cryptoisakmpkeepalive**

第 6 章

IPsec NAT 透過性

IPsec NAT 透過性機能では、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）の間における多くの既知の非互換性に対処することによって、ネットワーク内の NAT ポイントまたは PAT ポイントを経由して送信される IP セキュリティ（IPsec）のサポートが導入されています。

- 機能情報の確認，53 ページ
- IPsec NAT 透過性の制約事項，54 ページ
- IPsec NAT 透過性に関する情報，54 ページ
- NAT および IPsec の設定方法，59 ページ
- IPsec および NAT の設定例，62 ページ
- その他の参考資料，62 ページ
- IPsec NAT 透過性の機能情報，64 ページ
- 用語集，65 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPsec NAT 透過性の制約事項

この機能では、NAT および IPsec 間における多くの非互換性に対して対処が行われていますが、次の問題が依然として残されています。

インターネット キー交換（IKE）IP アドレスと NAT

この非互換性が問題になるのは、IP アドレスを、事前共有キーを検索するための検索キーとして使用する場合だけです。NAT またはリバース NAT によって IP 発信元アドレスまたは宛先アドレスが変更されると、IP アドレスと事前共有キーの間でミスマッチが生じます。

組み込み IP アドレスと NAT

ペイロードの完全性は保護されているので、NAT によって IPsec パケット内の IP アドレスを変換することが不可能です。組み込み IP アドレスを使用するプロトコルには、FTP、インターネット リレー チャット（IRC）、簡易ネットワーク管理プロトコル（SNMP）、Lightweight Directory Access Protocol（LDAP）、H.323、および Session Initiation Protocol（SIP）などがあります。

IPsec NAT 透過性に関する情報

IPsec NAT 透過性の利点

IPsec パケットの配信パス内に 1 つ以上の NAT または PAT ポイントがない場合、この機能を導入しなければ、標準の IPsec バーチャル プライベート ネットワーク（VPN）トンネルは動作しません。この機能によって NAT が IPsec 認識となり、その結果、リモート アクセス ユーザは、ホーム ゲートウェイへの IPsec トンネルを構築できます。

IPsec NAT Traversal の機能設計

IPsec NAT 透過性機能では、ユーザ データグラム プロトコル（UDP）ラッパ内に IPsec パケットをカプセル化することによって、NAT または PAT ポイントを通過する IPsec トラフィックのサポートが導入されており、その結果、パケットによる各 NAT デバイス間の通過が可能となっています。次の項では、NAT トラバーサルの詳細を定義します。

IKE フェーズ 1 ネゴシエーション：NAT 検出

インターネット キー エクスチェンジ（IKE）のフェーズ 1 ネゴシエーション中、IKE Quick Mode が開始される前に、NAT サポート、およびネットワーク パス上の NAT イグジスタンスという、2 つのタイプの NAT 検出が実行されます。

NAT サポートを検出するには、リモート ピアとベンダー ID ストリングを交換する必要があります。IKE フェーズ 1 のメイン モード（MM）1 および MM 2 の間、リモート ピアによって、ベン

ダー ID ストリング ペイロードが、そのピアに送信され、このバージョンでは NAT トラバーサルがサポートされていることが示されます。その後、ネットワーク パス上の NAT イグジスタンスを検出できます。

ネットワーク パス上に NAT が存在しているかどうかを検出すると、2 つのピア間のすべての NAT と、NAT の正確な位置がわかります。NAT デバイスによって、プライベート IP アドレスおよびポートがパブリック値に（またはパブリックからプライベートに）変換されます。パケットがデバイスを通過すると、この変換によって IP アドレスとポートが変更されます。ネットワーク パス上に NAT デバイスが存在しているかどうかを検出するには、ピアによって、各終端からの送信元アドレスと宛先アドレスの両方の IP アドレスおよびポートのハッシュを持つペイロードが送信される必要があります。両端でハッシュが計算され、ハッシュが一致した場合、各ピアによって、両ピア間におけるネットワーク パス上に NAT デバイスが存在しないことが認識されます。ハッシュが一致しない（つまり、誰かがアドレスまたはポートを変換した）場合、各終端では、NAT トラバーサルを実行し、ネットワークを介して IPsec パケットを取得する必要があります。

ハッシュは一連の NAT Discovery（NAT-D）ペイロードとして送信されます。各ペイロードには 1 つのハッシュが格納されます。複数のハッシュが存在する場合、複数の NAT-D が送信されます。ほとんどの環境では、NAT-D ペイロードは 2 つだけです。1 つは送信元 アドレスおよびポート用、もう 1 つは宛先アドレスおよびポート用です。最初に宛先 NA-D ペイロードが送信され、次に送信元 NAT-D ペイロードが送信されます。これは、受信側では、最初にローカル NAT-D ペイロードを処理し、次にリモート NAT-D ペイロードを処理することを予期する必要があることを意味します。メイン モードでは、NAT-D ペイロードは 3 番目および 4 番目のメッセージに格納され、アグレッシブ モード（AM）では、2 番目および 3 番目のメッセージ内に格納されます。

IKE フェーズ 2 ネゴシエーション：NAT トラバーサル決定

IKE フェーズ 1 による NAT サポート、およびネットワーク パス上の NAT イグジスタンスの検出中に、IKE フェーズ 2 によって両端の各ピアによって NAT トラバーサルが使用されるかどうかが決定されます。QM1 および QM2 におけるクイック モード（QM）セキュリティ アソシエーション（SA）ペイロードは、NAT トラバーサル ネゴシエーション用に使用されます。

NAT デバイスによって IP アドレスおよびポート番号が変更されるので、NAT と IPsec との間に非互換性が発生する可能性があります。そのため、元の送信元アドレスを交換することで、いかなる非互換性も回避できます。

NAT Traversal 用 IPsec パケットの UDP カプセル化

UDP カプセル化によって、IPsec パケットが NAT デバイスを経由できるようにするだけでなく、IPsec、NAT、および PAT 間における多くの非互換性問題に対処できます。解決できる問題は以下のとおりです。

IPsec ESP と PAT との間における非互換性：解決

PAT によって立法 IP アドレスおよびポートが検出されると、その PAT によって Encapsulating Security Payload（ESP）パケットが廃棄されます。このようなシナリオを防ぐために、UDP カプセル化が使用され、UDP ヘッダーの背後に ESP パケットが隠蔽されます。その結果、PAT によっ

て ESP パケットが UDP パケットとして扱われ、ESP パケットが通常の UDP パケットとして処理されます。

チェックサムと NAT との間における非互換性：解決

新しい UDP ヘッダー内では、チェックサムの値は必ずゼロに割り当てられます。この値によって、中間デバイスによるパケットのチェックサムを参照したチェックサムの確認が防止され、それにより、NAT によって IP 送信元アドレスおよび宛先アドレスが変更されるので、TCP UDP チェックサム問題が解決されます。

固定 IKE 宛先ポートおよび PAT 間における非互換性：解決

PAT によって、新しい変換用 UDP ヘッダー内のポート アドレスが変更され、元のペイロードは変更されないままとなります。

UDP カプセル化によってどのように IPSec パケットの送信が可能になるのかを確認するには、次の図を参照してください。

図 *2*：***NAT/PAT*** ポイントを介した標準的な ***IPsec*** トンネル（***UDP*** カプセル化なし）

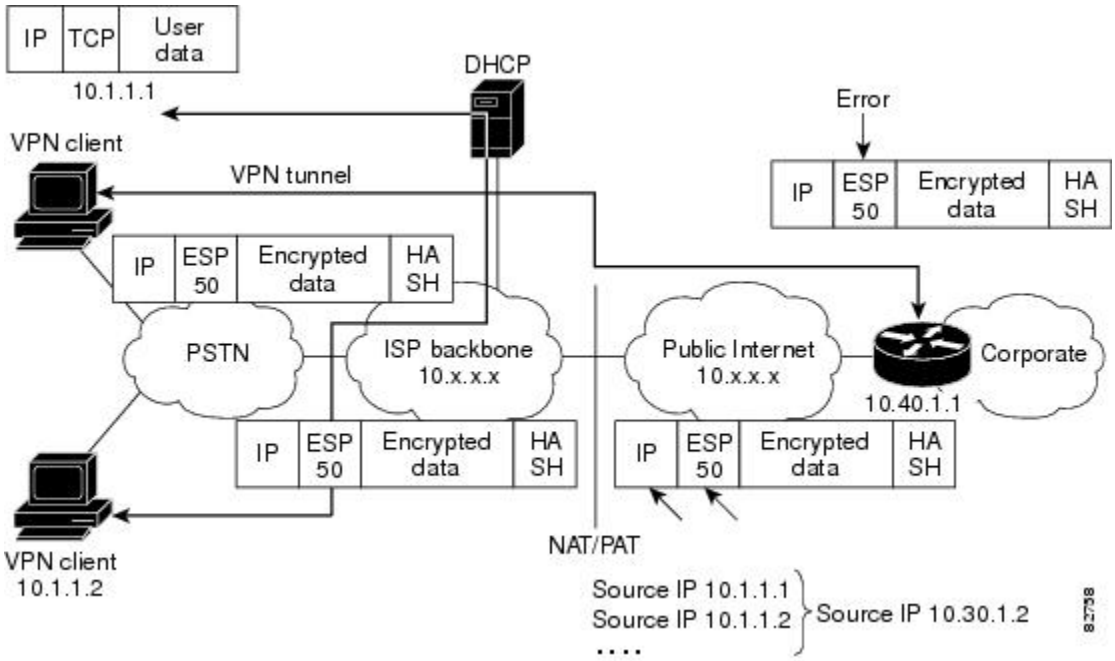
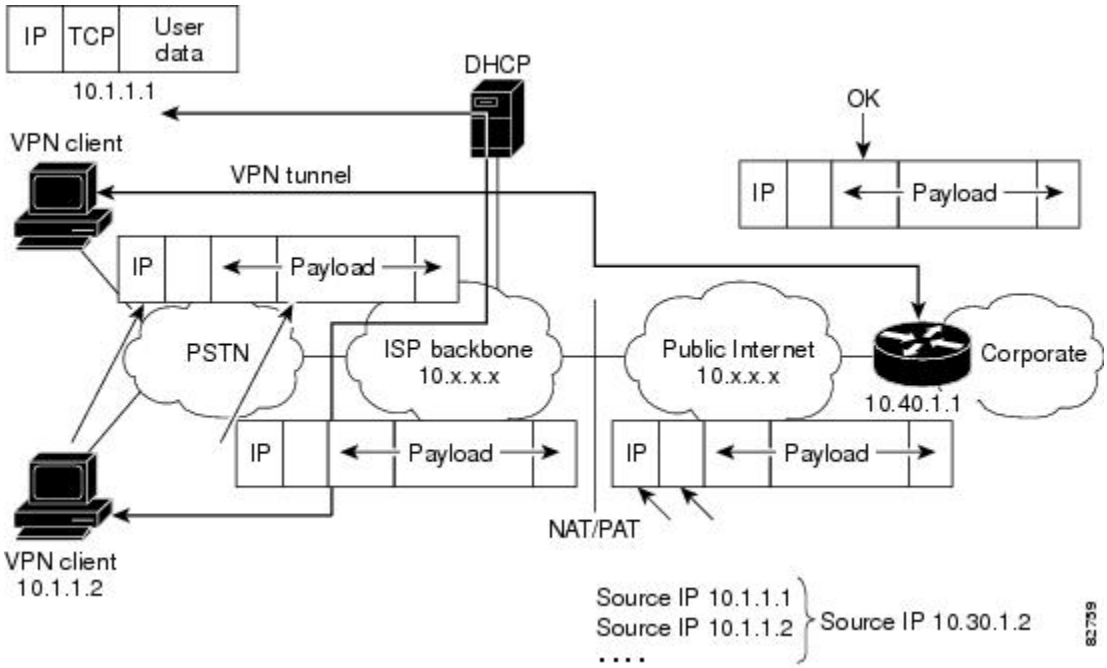


図 *3*：***UDP*** カプセル化を使用した ***IPsec*** パケット



ソフトウェア エンジン用 UDP カプセル化処理：トランスポート モードおよびトンネル モード EDP カプセル化

IPsec パケットがハードウェア アクセラレータまたはソフトウェア暗号化エンジンによって暗号化されると、UDP ヘッダーおよび非 IKE マーカ（長さは 8 バイト）が、元の IP ヘッダーと ESP ヘッダーの間に挿入されます。合計長フィールド、プロトコルフィールド、およびチェックサムフィールドはこの変更に合せて変更されます。次の 1 番目の図に、トランスポート モードが適用される前後の IPsec パケットを示します。2 番目の図には、トンネル モードが適用される前後の IPsec パケットを示します。

図 *4*：トランスポート モード：*ESP* カプセル化前後の *IPsec* パケット

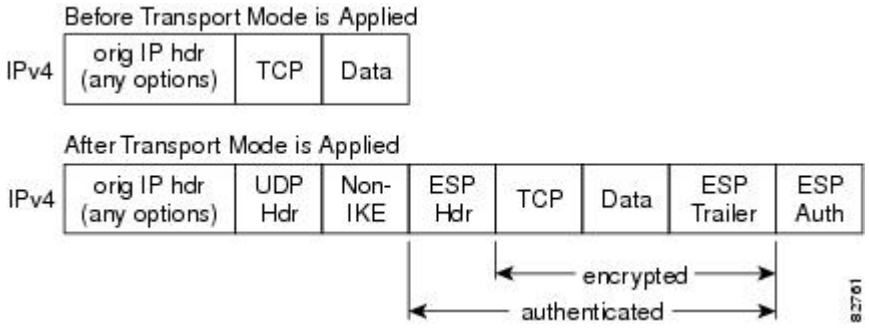
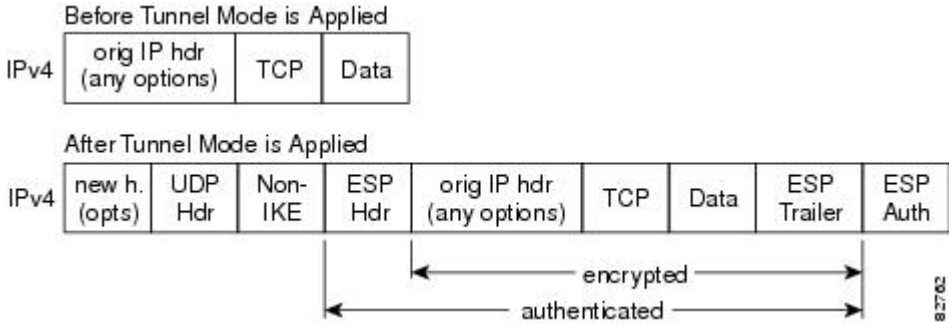


図 *5*：トンネル モード：*ESP* カプセル化前後の *IPsec* パケット



NAT キープアライブ

NAT キープアライブは、2 つのピア間の接続中におけるダイナミック NAT マッピングをアライブに保つためにイネーブルにされます。NAT キープアライブは、1 バイトの非暗号化ペイロードを持つ UDP パケットです。現在の Dead Peer Detection（DPD）実装は NAT キープアライブとほぼ同じですが、若干の違いがあります。DPD は、ピアのステータスを検出するために使用されます。一方、NAT キープアライブは、指定された期間（有効範囲は 5 ～ 3600 秒）にパケットが IPsec エンティティによって送信も受信されなかった場合に送信されます。

NAT キープアライブを（**crypto isakmp nat keepalive** コマンドを使用して）有効化する場合、アイドル値は NAT マッピングの有効期間（20 秒）より小さくなるようにする必要があります。

NAT および IPsec の設定方法

NAT Traversal の設定

NAT Traversal は、VPN デバイスによって自動検出される機能です。Cisco IOS XE Release 2.1 を実行するルータに設定するものはありません。両端の VPN デバイスが NAT-T 対応の場合、NAT Traversal が自動検出され、自動ネゴシエーションが行われます。

NAT Traversal の無効化

ご使用のネットワークですでに IPsec 認識 NAT が使用されている（spi マッチング スキーム）ことがわかっている場合、NAT トラバーサルをディセーブルにする必要が生じることがあります。NAT トラバーサルをディセーブルにするには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **nocryptoipsecnat-transparencyudp-encapsulation**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**nocryptoipsecnat-transparencyudp-encapsulation** 例： `Router(config)#`	NAT トラバーサルをディセーブルにします。

	コマンドまたはアクション	目的
	`no crypto ipsec nat-transparency udp-encapsulation`	

NAT キープアライブの設定

ルータを、NAT キープアライブを送信するように設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpnatkeepalive***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**cryptoisakmpnatkeepalive***seconds*
	
	例：
	
	`Router(config)#`
	`crypto isakmp nat keepalive 20`
		IPsec ノードによる NAT キープアライブ パケットの送信を可能にします。
		
		• *seconds*：キープアライブ パケット間の秒数。範囲は 5 ～ 3,600 秒。
		
		（注） タイマーが変更されると、インターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）SA のキープアライブが既存のタイマーに基づく場合、この秒数は SA ごとに変更されます。

	コマンドまたはアクション	目的
		（注） セキュリティ アソシエーションでキーの再生成の衝突が発生するのを防止するため、5%のジッタ メカニズム値がタイマーに適用されます。ピア ルータが多数あるときに、タイマーが低く設定されすぎている場合、ルータの CPU 使用率が高くなることがあります。

IPsec 設定の確認

設定を確認するには、次の任意の手順を実行します。

手順の概要

1. イネーブル化
2. **showcryptoipsecsa** [**map** *map-name* | **address** | **identity**] [**detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**showcryptoipsecsa** [**map** *map-name* | **address** | **identity**] [**detail** 例： `Router# show crypto ipsec sa`	現在の SA によって使用されている設定を表示します。

IPsec および NAT の設定例

NAT キープアライブの設定例

次に、NAT キープアライブを、20 秒毎に送信されるようにイネーブルにする方法の例を示します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 10.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
!
crypto map test2 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set t2
 match address 101
```

その他の参考資料

次の項では、IPsec NAT 透過性機能に関連した関連資料を示します。

関連資料

関連項目	マニュアル タイトル
その他の NAT 設定タスク	• 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Configuring NAT for IP Address Conservation」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Using Application Level Gateways with NAT」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Configuring NAT for High Availability」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Integrating NAT with MPLS VPNs」モジュール
その他の NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』

関連項目	マニュアル タイトル
その他の IPsec 設定タスク	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール
その他の IPsec コマンド	『Cisco IOS Security Command Reference』
IKE に関する情報	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IKE デッド ピア検出の追加情報	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Easy VPN Server」モジュール

標準

標準	Title
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC[1]	Title
RFC 2402	『IP Authentication Header』
RFC 2406	『IP Encapsulating Security Payload (ESP)』

[1] サポートされている RFC がすべて記載されているわけではありません。

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec NAT 透過性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *6*：*IPsec NAT* 透過性の機能情報

機能名	リリース	機能情報
IPsec NAT 透過性	Cisco IOS XE Release 2.1	IPsec NAT 透過性機能では、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）の間における多くの既知の非互換性に対処することによって、ネットワーク内の NAT ポイントまたは PAT ポイントを経由して送信される IP セキュリティ（IPsec）のサポートが導入されています。 次のコマンドが導入または変更されました。 **cryptoisamkpnatkeepalive**,**access-list**（**IP 拡張**）,**showcryptoipsecsa**

用語集

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）の略。Oakley キー交換や Skeme キー交換をインターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）フレームワーク内部に実装したハイブリッド プロトコルです。IKE は、他のプロトコルでも使用できますが、初期実装されるのは IPsec です。IKE は、IPsec ピアを認証し、IPsec キーをネゴシエーションし、IPsec セキュリティ アソシエーション（SA）を実行します。

IPsec：IP Security（IP セキュリティ）の略。インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

NAT：Network Address Translation（ネットワーク アドレス変換）の略。企業内で使用されているプライベート IP アドレスを、インターネットなど企業外で使用される、ルーティング可能なパブリック アドレスに変換します。NAT は、アドレスのプライベートからパブリックへの 1 対 1 のマッピングと見なされます。

PAT：Port Address Translation（ポート アドレス変換）の略。NAT と同様、PAT でもプライベート IP アドレスからルーティング可能なパブリック アドレスへの変換が行われます。NAT とは異なり、PAT では、プライベート アドレスのパブリック アドレスへの多対 1 のマッピングが提供されます。パブリック アドレスの各インスタンスは、一意性を確保するために特定のポート番号と関連付けられます。PAT は、一連のパブリック アドレスを取得するコストが組織にとって高すぎるような環境で使用可能です。

第 7 章

IPsec トンネルを使用する DF ビット オーバーライド機能

IPsec トンネル機能による DF ビット オーバライド機能では、トンネル モード IPsec トラフィックを、グローバル レベルまたは各インターフェイス レベルでカプセル化する際に、DF ビットを設定できます。したがって、ルータが DF ビットを消去するように設定されている場合、ルータは、元の DF のパケット設定に関係なく、パケットを断片化できます。

- 機能情報の確認，67 ページ
- IPsec トンネルを使用する DF ビット オーバーライド機能の前提条件，68 ページ
- IPsec トンネルを使用する DF ビット オーバーライド機能の制約事項，68 ページ
- IPsec トンネルを使用する DF ビット オーバーライド機能に関する情報，68 ページ
- IPsec トンネルを使用する DF ビット オーバーライド機能の設定方法，69 ページ
- IPsec トンネルを使用する DF ビット オーバーライド機能の設定例，70 ページ
- その他の参考資料，71 ページ
- IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報，73 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPsec トンネルを使用する DF ビット オーバーライド機能の前提条件

ルータで IPsec がイネーブルに設定されている必要があります。

IPsec トンネルを使用する DF ビット オーバーライド機能の制約事項

パフォーマンス上の影響

各パケットがプロセス レベルで再アセンブルされるため、高いデータ レートでパフォーマンスに大きな影響が生じます。主な警告事項には、次の 2 つがあります。

- 再アセンブル キューが満杯になると、フラグメントが強制的に廃棄されることがあります。
- プロセス スイッチングにより、トラフィックの速度は低下します。

DF ビットの設定要件

複数のインターフェイスがローカル アドレス機能を使用して同じクリプト マップを共有する場合、これらのインターフェイスは同じ DF ビット設定を共有する必要があります。

機能のアベイラビリティ

この機能は IPsec トンネル モードだけで使用できます（IPsec トランスポート モードは、カプセル化 IP ヘッダーを提供しないので、影響を受けません）。

IPsec トンネルを使用する DF ビット オーバーライド機能に関する情報

機能の概要

IPsec トンネル機能による DF ビット オーバライド機能により、ルータがカプセル化ヘッダーの Don't Fragment（DF）ビットをクリア、設定、またはコピーするかどうかを指定できます。DF ビットは IP ヘッダー内のビットで、このビットは、ルータがパケットを断片化することを許可されているかどうか判別します。

一部のユーザ設定のホストでは、次の機能を実行します。

- 送信されたパケットに DF ビットを設定する。

- ファイアウォールを使用して、ファイアウォールの外部からくるインターネット制御メッセージ プロトコル（ICMP）エラーをブロックし、ホストがファイアウォールの外部から最大伝送単位（MTU）サイズを認識できないようにする。
- IP セキュリティ（IPsec）を使用してパケットをカプセル化し、MTU サイズを縮小する。

使用可能な MTU サイズを認識できないようにホストが設定されている場合、DF ビットをクリアし、パケットを断片化するよう、ルータを設定できます。

（注） この機能は、RFC 2401 に準拠して、グローバルに、またはインターフェイスごとに設定できます。両方のレベルを設定すると、インターフェイス コンフィギュレーションにより、グローバル コンフィギュレーションが上書きされます。

IPsec トンネルを使用する DF ビット オーバーライド機能の設定方法

トンネル モードでのカプセル化ヘッダーへの DF ビットの設定

トンネル モードで DF ビットをカプセル化ヘッダーに設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoipsecdf-bit** [**clear** | **set** | **copy**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**cryptoipsecdf-bit** [**clear** | **set** | **copy**] 例： `Router (config)# crypto ipsec df-bit set`	すべてのインターフェイスのトンネル モードで DF ビットをカプセル化ヘッダーに設定します。 指定されたインターフェイスに DF ビットを設定するには、インターフェイス コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。 （注） DF ビットインターフェイス コンフィギュレーション設定によって、すべての DF ビット グローバル コンフィギュレーション設定が上書きされます。

DF ビット設定の確認

ルータ上の現在の DF ビット設定を確認するには、 **show running-config** コマンドを EXEC モードで使用します。

IPsec トンネルを使用する DF ビット オーバーライド機能の設定例

DF ビットの設定例

次の例では、DF ビットの設定をグローバルに消去し、DF ビットを FastEthernet というインターフェイスにコピーするようにルータが設定されています。したがって、FastEthernet 以外のすべてのインターフェイスでは、ルータは使用可能な MTU サイズより大きいパケットを送信でき、FastEthernet では、ルータはパケットをフラグメント化できます。

```
crypto isakmp policy 1
   hash md5
   authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set exampleset ah-md5-hmac esp-des
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set exampleset
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set exampleset
```

```
match address 102
!
!
interface FastEthernet
   ip address 192.168.10.38 255.255.255.0
   ip broadcast-address 0.0.0.0
   media-type 10BaseT
   crypto map armadillo
   crypto ipsec df-bit copy
!
interface FastEthernet1
   ip address 192.168.11.75 255.255.255.0
   ip broadcast-address 0.0.0.0
   media-type 10BaseT
   crypto map basilisk
!
interface Serial0
   no ip address
   ip broadcast-address 0.0.0.0
   no ip route-cache
   no ip mroute-cache
```

その他の参考資料

次のセクションには、IPsec トンネル機能による DF ビット オーバライド機能の関連資料が記載されています。

関連資料

関連項目	マニュアル タイトル
インターネットキーエクスチェンジネットワークと IPsec ネットワーク	「Configuring Internet Key Exchange for IPsec VPNs」
IPSec ネットワークのコマンド	『Cisco IOS Security Command Reference』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 7：***IPsec* トンネルを使用する *DF* ビット オーバーライド機能の機能情報**

機能名	リリース	機能情報
IPsec トンネルを使用する DF ビット オーバーライド機能	Cisco IOS XE Release 2.1	この機能により、ルータがカプセル化ヘッダーから Don't Fragment（DF）ビットを消去、設定、またはコピーするかどうかを指定できます。DF ビットは IP ヘッダー内のビットで、このビットは、ルータがパケットを断片化することを許可されているかどうか判別します。 次のコマンドが導入または変更されました。**cryptoipsecdf-bit**

第 8 章

IPsec SA アイドル タイマー

Cisco IOS XE ソフトウェアを実行しているルータによってピアの IPsec セキュリティ アソシエーション（SA）が作成される場合、その SA を維持するためにリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。IPsec SA アイドル タイマー機能では、SA のアクティビティをモニタリングするための、設定可能なアイドル タイマーが導入されており、これにより、アイドル状態のピアの SA を削除できます。この機能には、次のような利点があります。

- 向上したリソースの可用性
- Cisco IOS XE IPSec 配置のスケーラビリティの向上この機能によって、アイドル状態のピアによるリソースの浪費を防止できるので、より多くのリソースを、必要に応じた新しい SA の作成に使用できます。

- 機能情報の確認，75 ページ
- IPsec セキュリティ アソシエーション アイドル タイマーの前提条件，76 ページ
- IPsec セキュリティ アソシエーション アイドル タイマーに関する情報，76 ページ
- IPsec セキュリティ アソシエーション アイドル タイマーの設定方法，77 ページ
- IPsec セキュリティ アソシエーション アイドル タイマーの設定例，79 ページ
- その他の参考資料，79 ページ
- IPsec セキュリティ アソシエーション アイドル タイマーの機能仕様，81 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPsec セキュリティ アソシエーション アイドル タイマーの前提条件

インターネット キー エクスチェンジ（IKE）は、『*Cisco IOS XE Security Configuration Guide*』の「Configuring Internet Key Exchange Security Protocol」の章に従って設定する必要があります。

IPsec セキュリティ アソシエーション アイドル タイマーに関する情報

IPsec セキュリティ アソシエーションのライフタイム

現在、Cisco IOS ソフトウェアでは、IPsec SA のライフタイムの設定が可能です。ライフタイムは、グローバルに、またはクリプト マップごとに設定できます。ライフタイムには、「指定時刻」ライフタイムと「トラフィック量」ライフタイムの 2 つがあります。これらのライフタイムに到達すると、セキュリティ アソシエーションが期限切れになります。

IPsec SA アイドル タイマー

IPsec SA アイドル タイマーは、IPsec SA のグローバル ライフタイムとは異なります。グローバル ライフタイムの有効期間は、ピアのアクティビティとは独立しています。IPsec SA アイドル タイマーを使用すれば、非アクティブなピアに関連付けられた SA を、グローバル ライフタイムが期限切れになる前に削除できます。

IPsec SA アイドル タイマーが設定されていない場合、IPsec SA のグローバル ライフタイムだけが適用されます。SA は、ピアのアクティビティと関わりなく、グローバル タイマーが有効期限切れになるまで維持されます。

（注） アイドル タイマーの期限切れのために、特定のピアに対する最新の IPsec SA が削除された場合、そのピアに対する IKE も削除されます。

IPsec セキュリティ アソシエーション アイドル タイマーの設定方法

IPSec SA アイドル タイマーのグローバルな設定

このタスクでは、IPsec SA アイドル タイマーをグローバルに設定します。このアイドル タイマーの設定は、すべての SA に適用されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoipsecsecurity-associationidle-time***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoipsecsecurity-associationidle-time***seconds* 例： `Router(config)# crypto ipsec security-association idle-time 600`	IPsec SA アイドル タイマーを設定します。 • *seconds* 引数では、アイドル タイマーが非アクティブ ピアによる SA の維持を許可する時間を秒単位で指定します。*seconds* 引数の有効な値の範囲は 60 ～ 86400 です。

IPSec SA アイドル タイマーのクリプト マップ単位での設定

このタスクでは、指定されたクリプトマップの IPsec SA アイドル タイマーを設定します。アイドル タイマーの設定は、指定されたクリプト マップ下のすべての SA に適用されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptomap***map-nameseq-number***ipsec-isakmp**
4. **setsecurity-associationidle-time***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptomap***map-nameseq-number***ipsec-isakmp** 例： `Router(config)# crypto map test 1 ipsec-isakmp`	クリプトマップエントリを作成または変更し、クリプトマップ コンフィギュレーション モードを開始します。
ステップ 4	**setsecurity-associationidle-time***seconds* 例： `Router(config-crypto-map)# set security-association idle-time 600`	デフォルト ピアが使用される前に、現在のピアをアイドル状態にしておける最大期間を指定します。 • *seconds* 引数は、デフォルト ピアが使用される前に現在のピアをアイドル状態にできる秒数です。有効値は 60 ～ 86400 です。

IPsec セキュリティ アソシエーション アイドル タイマーの設定例

IPsec SA アイドル タイマー のグローバル設定例

次に、IPsec SA アイドル タイマー をグローバルに設定して、600 秒後に非アクティブなピアの SA を廃棄している例を示します。

```
crypto ipsec security-association idle-time 600
```

暗号マップごとの IPsec SA アイドル タイマーの設定例

次に、test という名前のクリプト マップの IPsec SA アイドル タイマーを設定して、600 秒後に非アクティブなピアの SA を廃棄している例を示します。

```
crypto map test 1 ipsec-isakmp
 set security-association idle-time 600
```

その他の参考資料

ここでは、IPsec セキュリティ アソシエーション アイドル タイマー機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IKE の設定に関する追加情報	「Internet Key Exchange for IPsec VPNs」
IPsec SA のグローバル ライフタイムの設定に関する追加情報	• IPsec を使用した VPN のセキュリティの設定 • IPSEC 優先ピア
追加セキュリティ コマンド	『Cisco IOS Security Command Reference』

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	---

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec セキュリティ アソシエーション アイドル タイマーの機能仕様

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *8* : ***IPsec*** セキュリティ アソシエーション アイドル タイマーの機能仕様

機能名	リリース	機能情報
IPsec SA アイドル タイマー	Cisco IOS XE Release 2.1	Cisco IOS XE ソフトウェアを実行しているルータによってピアの IPsec セキュリティ アソシエーション（SA）が作成される場合、その SA を維持するためにリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。IPsec SA アイドル タイマー機能では、SA のアクティビティをモニタリングするための、設定可能なアイドル タイマーが導入されており、これにより、アイドル状態のピアの SA を削除できます。 次のコマンドが導入または変更されました。 **cryptoipsecsecurity-associationidle-time**
	Cisco IOS XE Release 2.1	**setsecurity-associationidle-time** コマンドが追加され、指定された暗号マップに対する IPsec アイドル タイマーの設定が可能になりました。 次のコマンドが導入または変更されました。 **setsecurity-associationidle-time**

第 9 章

IPv6 IPsec の QoS

IPv6 IPsec QoS 機能は、Quality of Service（QoS）ポリシーを IPv6 IPsec に適用できるようにします。

- 機能情報の確認，83 ページ
- IPv6 IPsec QoS に関する情報，84 ページ
- IPv6 IPsec QoS の設定方法，84 ページ
- QoS の設定例，89 ページ
- IPv6 IPsec QoS の追加情報，91 ページ
- IPv6 IPsec QoS の機能情報，92 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPv6 IPsec QoS に関する情報

IPv6 IPsec QoS の概要

IPv6 IPsec QoS 機能は、IPv6 IPsec に Quality of Service（QoS）ポリシーを適用します。この機能は、次の機能をサポートしています。

- Crypto LLQ QoS：従来の Cisco モジュラ QoS CLI（MQC）の QoS 設定（PAK_PRIORITY など）により QoS に分類されて優先度レベル 1 または 2 にマークされたトラフィックがエンキューされ、暗号プロセッサの前にプライオリティ キューに入れられます。IPsec 暗号化エンジンの低遅延キューイング（LLQ）により、プライオリティ トラフィックのパケット遅延を軽減できます。
- IPsec QoS Pre-Classify：QoS Pre-Classify が暗号マップの下で設定されることで、暗号化の前に IPSec で元のレイヤ 3 およびレイヤ 4 ヘッダーを保存できるようにします。これにより QoS では、保存されたヘッダーを使用した分類ができます。
- QoS group-based LLQ：QoS group-based LLQ 機能により、IPsec で LLQ QoS グループの設定を確認することで、パケットが低遅延キューイング（LLQ）にエンキューされる前に高プライオリティ パケットであるかどうかを判断できます。

IPv6 IPsec QoS の設定方法

Crypto LLQ QoS の設定

IPsec と QoS が物理インターフェイスに設定され、QoS ポリシーにプライオリティ クラスがある場合、IPSec はインターフェイスにアタッチしたポリシーに基づいてパケットを分類します。プライオリティ クラスに一致するパケットを低遅延キューにエンキューします。優先順位の高いパケットは低遅延キューイング（LLQ）にエンキューされます。

このタスクを実行して、サービス ポリシーを出力インターフェイスにアタッチし、IPsec 暗号化エンジンの LLQ を有効化します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***physical-interface-name*
4. **ipv6 address***{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}*
5. **service-policy output***policy-map*
6. **ipv6 crypto map***map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***physical-interface-name* 例： `Device(config)# interface GigabitEthernet0/0/1`	IPsec 暗号化エンジンの LLQ を使ってインターフェイスを指定します。
ステップ 4	**ipv6 address***{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}* 例： `Device(config-if)# ipv6 address 2001:DB8:FFFF::2/64`	インターフェイスで IPv6 アドレスを設定します。
ステップ 5	**service-policy output***policy-map* 例： `Device(config-if)# service-policy output p1`	指定したサービス ポリシー マップを出力インターフェイスにアタッチし、IPsec暗号化エンジンのLLQをイネーブルにします。
ステップ 6	**ipv6 crypto map***map-name* 例： `Device(config-if)# ipv6 crypto map CMAP_1`	インターフェイスで IPv6 暗号マップを有効化します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

QoS Pre-classify の設定

暗号マップ上での Pre-classify の設定

qos pre-classify コマンドは暗号マップに適用され、トンネル単位の設定が可能です。QoS ポリシーは、暗号化の前に、L3 および L4 ヘッダーに基づいて、パケットに適用されます。

このタスクを実行して、QoS Pre-classify を暗号マップに適用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6cryptomap***map-name*
4. **qospre-classify**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6cryptomap***map-name* 例： `Device(config-if)# ipv6 crypto map CM_V6`	暗号マップ コンフィギュレーション モードを開始し、設定する暗号マップを指定します。
ステップ 4	**qospre-classify** 例： `Device(config-if)# qos pre-classify`	QoS Pre-classify を暗号マップで有効化します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トンネル インターフェイス上での Pre-classify の設定

qos pre-classify コマンドは、IPv6 IPsec トンネル インターフェイスに適用され、QoS で設定オプションをトンネル単位にします。

このタスクを実行して、QoS Pre-classify をトンネル インターフェイスに適用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***tunnel-interface-name*
4. **ipv6 address***{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}*
5. **qospre-classify**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***tunnel-interface-name* 例： `Device(config)# interface Tunnel1`	インターフェイス コンフィギュレーション モードを開始して、設定するトンネルまたは仮想インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 address***{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}* 例： `Device(config-if)# ipv6 address 2001:DB8:FFFF::2/64`	インターフェイスで IPv6 アドレスを設定します。
ステップ 5	**qospre-classify** 例： `Device(config-if)# qos pre-classify`	QoS Pre-classify をトンネル インターフェイスで有効化します。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

LLQ QoS グループの設定

platform ipsec llq qos-group コマンドは、このコマンドで設定される QoS グループに一致するトラフィックの低遅延キューイングを有効化します。

このタスクを実行して、QoS グループの LLQ を有効化します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **platformipsecllqqos-group***group-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platformipsecllqqos-group***group-number* 例： `Device(config)# platform ipsec llq qos-group 1`	LLQ を有効化する QoS グループを指定します。有効値は 1 ～ 99 です。
ステップ 4	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

QoS の設定例

例：Crypto LLQ QoS の設定

次の例では、出力インターフェイスに対してサービスポリシーマップを指定し、インターフェイスで IPv6 暗号マップを有効にする方法を示します。

```
!
class-map match-all c2
  match precedence 5  6  7
class-map match-all c1
  match precedence 0  1  2  3

policy-map p1
  class c1
    priority percent 10
  class c2
    bandwidth remaining percent 3

crypto map ipv6 CMAP_1 1 ipsec-isakmp
  set peer address 2001:DB8:FFFF::1
  set transform-set ESP-3DES-SHA
  match address 102

interface GigabitEthernet0/0/1
  ipv6 address 2001:DB8:FFFF::2/64
  ipv6 crypto map CMAP_1
  service-policy output p1
```

例：暗号マップ上での Pre-classify の設定

次の例では、暗号マップ CM_V6 で **qos pre-classify** コマンドを使用して QoS 事前分類を有効化する方法を示します。

```
!
crypto map ipv6 CM_V6 10 ipsec-isakmp
  match address ACL_IPV6_1
  set transform-set set1
  set peer 2001:DB8:FFFF::1
  qos pre-classify
!
interface GigabitEthernet0/0/1
  ipv6 address 2001:DB8:FFFF::2/64
  service-policy output policy1
  ipv6 crypto map CM_V6
```

例：トンネル インターフェイス上での Pre-classify の設定

次の例では、トンネル インターフェイス tunnel1 で **qos pre-classify** コマンドを使用して QoS 事前分類を有効化する方法を示します。

```
interface GigabitEthernet1/1/2
  ipv6 address 2001:DB8:1::F/64
  service-policy output policy1
!
interface Tunnel1
  ipv6 address 2001:DB8:2::F/64
  qos pre-classify
  ipv6 mtu 1400
  tunnel protection ipsec profile greprof
```

例：LLQ QoS グループの設定

次の例では、QoS グループで低遅延キューイングを設定する方法を示します。

```
!
platform ipsec llq qos-group 1
platform ipsec llq qos-group 49
!
!
crypto map ipv6 cmap 1 ipsec-isakmp
  set peer 2001:DB8:FFFF:1::E/64
  set security-association lifetime seconds 600
  set transform-set aes-192
  match address 102
!
!
class-map match-all c1
  match precedence 5
class-map match-all c2
  match precedence 2
class-map match-all c3
  match precedence 4
class-map match-all c4
  match precedence 3
!
policy-map p1
  class c3
```

```
    set qos-group 20
  class c1
    set qos-group 49
  class c4
    set qos-group 77
!
policy-map p2
  class class-default
    set qos-group 1
!
interface GigabitEthernet0/2/0
  ipv6 address
  negotiation auto
  cdp enable
  ipv6 crypto map cmap
  service-policy input p2
!
!
interface GigabitEthernet0/2/7
  ipv6 address 2001:DB8:FFFF:1::F/64
  negotiation auto
  cdp enable
  service-policy input p1
!
```

IPv6 IPsec QoS の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
IPv6 コマンド	IPv6 コマンド リファレンス
QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』

シスコのテクニカル サポート

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

IPv6 IPsec QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *9* : ***IPv6 IPsec QoS*** の機能情報

機能名	リリース	機能情報
IPv6 IPsec QoS	15.4(1)S	IPv6 IPsec QoS 機能は、QoS ポリシーを IPv6 IPsec に適用できるようにします。この機能は、次の機能をサポートしています。 • Crypto LLQ QoS • IPsec QoS Pre-Classify • QoS group-based LLQ 次のコマンドが変更されました。**ipv6cryptomap**

第 10 章

IPv6 仮想トンネル インターフェイス

シスコのネットワーク デバイス用の Cisco IOS IPv6 セキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

Cisco IOS IPsec 機能では、IP パケット レベルのネットワーク データ暗号化を利用して、標準規格に準拠した堅牢なセキュリティが提供されています。また、IPsec では、データ機密保持サービスだけでなく、データ認証およびリプレイ攻撃防止サービスも提供されています。

IPsec は、IPv6 仕様の必須コンポーネントです。IPv6 ユニキャストおよびマルチキャスト トラフィックを保護するために、IPv6 IPsec トンネル モードおよびカプセル化が使用されます。このマニュアルでは IPv6 セキュリティへの IPsec の実装について説明します。

- 機能情報の確認，93 ページ
- IPv6 仮想トンネル インターフェイスに関する情報，94 ページ
- IPv6 仮想トンネル インターフェイスの設定方法，96 ページ
- IPv6 仮想トンネル インターフェイスの設定例，108 ページ
- その他の参考資料，109 ページ
- IPv6 仮想トンネル インターフェイスの機能情報，110 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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

IPv6 仮想トンネル インターフェイスに関する情報

IPsec for IPv6

IP セキュリティ（IPsec）は Internet Engineering Task Force (IETF)によって開発されたオープン規格のフレームワークであり、インターネットなどの保護されていないネットワークを介して機密情報を送信する際のセキュリティを確保します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。IPsec は、次のオプションのネットワーク セキュリティ サービスを提供します一般に、ローカル セキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます。

- データ機密性：IPsec 送信者はネットワークを通じてパケットを送信する前に、パケットを暗号化できます。
- データ整合性：IPSec 受信者は、IPSec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないようにします。
- データ送信元認証：IPSec 受信者は、送信された IPSec パケットの送信元を認証できます。このサービスはデータ整合性サービスに依存します。
- アンチ リプレイ：IPsec 受信者はリプレイされたパケットを検出し、拒否できます。

IPsec を使用すれば、データを、観測、変更、またはスプーフィングされることなく、パブリック ネットワークを介して送信できます。IPsec 機能は IPv6 と IPv4 の両方で似ていますが、サイト間トンネル モードは IPv6 だけでサポートされています。

IPv6 では、IPsec は AH 認証ヘッダーと ESP 拡張ヘッダーを使用して実装されます。認証ヘッダーは、送信元の整合性と認証を提供します。再送されたパケットに対するオプションの保護も提供します。認証ヘッダーによって、ほとんどの IP ヘッダーフィールドの整合性が保護され、シグニチャベースのアルゴリズムに従って送信元が認証されます。ESP ヘッダーは、機密性、送信元の認証、内部パケットのコネクションレス型整合性、アンチリプレイ、および制限されたトラフィック フローの機密性を提供します。

インターネット キー交換（IKE）プロトコルとは、IPsec とともに使用されるキー管理プロトコル標準です。IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

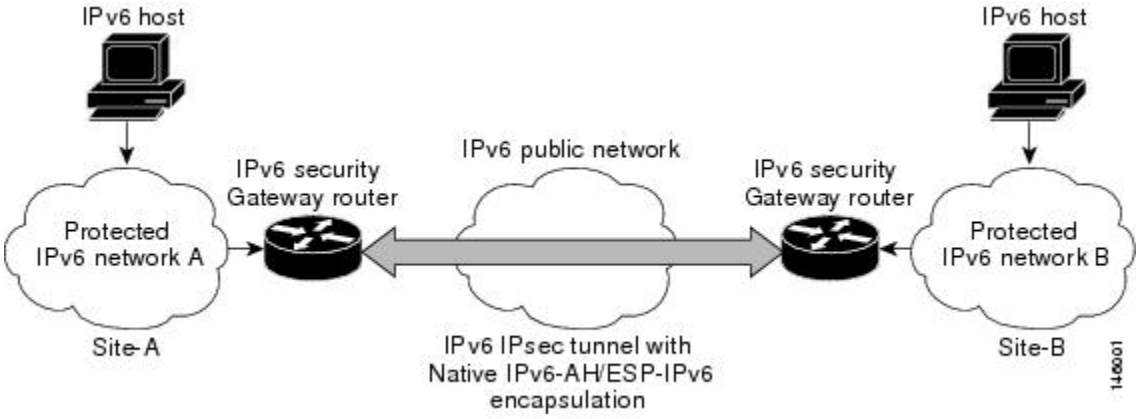
IKE は、Oakley キー交換や Skeme キー交換を Internet Security Association Key Management Protocol（ISAKMP）フレームワークの内部に実装したハイブリッドプロトコルです（ISAKMP、Oakley、および Skeme は IKE によって実装されるセキュリティ プロトコルです）。次の図を参照してください。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護

IPsec 仮想トンネル インターフェイス（VTI）は、IPv6 トラフィックのサイト間 IPv6 暗号保護を提供します。IPv6 ユニキャストと IPv6 マルチキャストのあらゆるタイプのトラフィックを保護するために、ネイティブ IPv6 IPsec カプセル化が使用されます。

IPsec VTI では、IPv6 ルータがセキュリティ ゲートウェイとして機能し、他のセキュリティ ゲートウェイ ルータ間に IPsec トンネルを確立したり、トラフィックが内部ネットワークからパブリック IPv6 インターネットを介して送信された場合に暗号 IPsec 保護を提供したりできます（次の図を参照）。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

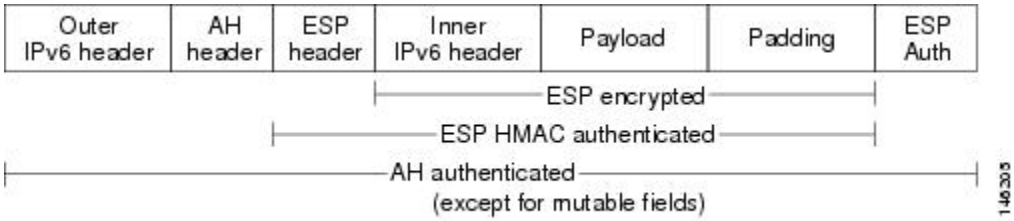
図 *6*：*IPv6* の *IPsec* トンネル インターフェイス



IPsec トンネルを設定すると、トンネルインターフェイスの回線プロトコルがアップ状態に変わる前に、IKE および IPsec セキュリティ アソシエーション（SA）がネゴシエーションされ、設定されます。リモート IKE ピアは、トンネルの宛先アドレスと同じです。ローカル IKE ピアは、トンネルの宛先アドレスと同じ IPv6 アドレス スコープを持つトンネルの送信元インターフェイスから選択されたアドレスです。

次の図に、IPsec パケット形式を示します。

図 *7*：*IPv6 IPsec* パケット形式



IPv6 仮想トンネル インターフェイスの設定方法

サイト間 IPv6 IPsec 保護用の VTI の設定

IPv6 での IKE ポリシーおよび事前共有キーの定義

IKE ネゴシエーションは保護する必要があるため、各 IKE ネゴシエーションは、共有（共通）の IKE ポリシーについて両ピアが同意することで開始されます。このポリシーには、次の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータとピアの認証方法を記述します。

両ピアがポリシーに同意すると、各ピアに確立されている SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーションにおける以降すべての IKE トラフィックに適用されます。

パラメータ値の組み合わせをそれぞれ変えることにより各ピアにプライオリティをつけたポリシーを複数設定できます。ただし、そのうちの少なくとも 1 つのポリシーには、リモート ピアのポリシーのいずれかとまったく同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値が設定されている必要があります。作成する各ポリシーに対して、一意のプライオリティを割り当てます（1 ～ 10,000 で指定し、1 が最大のプライオリティ）。

（注） サポートされているパラメータの値が1つしかないデバイスを使用する場合は、もう一方のデバイスでサポートされている値を設定する必要があります。この制限を別にすれば、セキュリティとパフォーマンスには通常トレードオフの関係があり、パラメータ値の多くにはこのトレードオフがあります。ネットワークのセキュリティ リスクのレベルと、そのリスクに対する許容度を評価する必要があります。

IKE ネゴシエーションが開始されると、IKE は、両方のピアにある同じ IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、自分のプライオリティ 1 位のポリシーと、相手のピアから受け取ったポリシーを比較し、一致するポリシーを探します。一致するポリシーが見つかるまで、リモート ピアは優先順位が高い順に各ポリシーをチェックします。

2 つのピアのポリシーが一致するのは、両方のピアが同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値を持ち、リモート ピアのポリシーに指定されているライフタイムが、比較対象のポリシーのライフタイム以下の場合です（ライフタイムが同一でない場合は、リモート ピアのポリシーでの、より短いライフタイムが使用されます）。

一致した場合は、IKE がネゴシエーションを完了し、IPsec セキュリティ アソシエーションが作成されます。一致するポリシーが見つからなかった場合は、IKE はネゴシエーションを拒否し、IPsec は確立されません。

（注） ポリシーに指定する認証方式によっては、追加の設定が必要な場合があります。ピアのポリシーに必要な関連設定がされていないと、一致するポリシーをリモート ピアで検索するときに、ピアはポリシーを送信しません。

IKE ポリシーで事前共有キーを使用するピアそれぞれについて ISAKMP ID を設定する必要があります。

2 つのピアが IKE を使って IPsec SA を確立する場合、各ピアが自分の ID をもう一方のピア（リモート ピア）に送信します。各ピアは、ルータの ISAKMP ID の設定に従い、ホスト名または IPv6 アドレスを送信します。

デフォルトでは、ピアの ISAKMP ID はピアの IPv6 アドレスになっています。必要に応じて ID をピアのホスト名に変更します。一般的に、すべてのピアの ID は同じ設定（すべてのピアで IPv6 アドレスを設定するか、すべてのピアでホスト名を設定）にします。お互いの識別にホスト名を使うピアと IPv6 アドレスを使うピアが混在していると、リモート ピアの ID が識別されない場合に DNS lookup で ID を解決できなくなり、IKE ネゴシエーションが失敗することがあります。

このタスクを実行して、IPv6 での IKE ポリシーおよび事前共有キーを作成します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmppolicy***priority*
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **hash** {**sha** | **md5**}
6. **group** {**1** | **2** | **5**}
7. **encryption** {**des** | **3des** | **aes** | **aes192** | **aes256**}
8. **lifetime***seconds*
9. **exit**
10. **cryptoisakmpkey** password-type keystring *keystring{***address***peer-address*| **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname***hostname}[***no-xauth***]*
11. **cryptokeyring***keyring-name* [**vrf***vrf-name*]
12. **pre-shared-key** {**address***address* [*mask*] | **hostname***hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key***key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmppolicy***priority* 例： `Router(config)# crypto isakmp policy 15`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。 • ポリシー番号 1 は、最もプライオリティが高いポリシーを示します。*priority* 引数の値が小さいほど、プライオリティは高くなります。
ステップ 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} 例： `Router(config-isakmp-policy)# authentication pre-share`	IKE ポリシー内の認証方式を指定します。 • **rsa-sig** キーワードと **rsa-encr** キーワードは IPv6 でサポートされていません。
ステップ 5	**hash** {**sha** | **md5**} 例： `Router(config-isakmp-policy)# hash md5`	IKE ポリシー内のハッシュ アルゴリズムを指定します。
ステップ 6	**group** {**1** | **2** | **5**} 例： `Router(config-isakmp-policy)# group 2`	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 7	**encryption** {**des** | **3des** | **aes** | **aes192** | **aes256**} 例： `Router(config-isakmp-policy)# encryption 3des`	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 8	**lifetime***seconds* 例： `Router(config-isakmp-policy)# lifetime 43200`	IKE SA のライフタイムを指定します。 • IKE ライフタイム値の設定は任意です。
ステップ 9	**exit** 例： `Router(config-isakmp-policy)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**cryptoisakmpkey** password-type keystring *keystring{***address***peer-address*| **ipv6** {*ipv6-address*|*ipv6-prefix*} | **hostname***hostname}[***no-xauth***]* 例： `Router(config)# crypto isakmp key 0 my-preshare-key-0 address ipv6 3ffe:1001::2/128`	事前共有認証キーを設定します。
ステップ 11	**cryptokeyring***keyring-name* [**vrf***vrf-name*] 例： `Router(config)# crypto keyring keyring1`	IKE 認証で使用される暗号キーリングを定義し、config-keyring モードを開始します。
ステップ 12	**pre-shared-key** {**address***address* [*mask*] | **hostname***hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key***key* 例： `Router (config-keyring)# pre-shared-key ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	IKE 認証に使用する事前共有キーを定義します。

ISAKMP アグレッシブ モードの設定

一般的には、サイト間シナリオではアグレッシブ モードを設定する必要はありません。通常、デフォルト モードが使用されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmppeer** {**address** {*ipv4-address* | **ipv6***ipv6-addressipv6-prefix-length*} | **hostname***fqdn-hostname*}
4. **setaggressive-modeclient-endpoint**{*client-endpoint* | **ipv6***ipv6-address*}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmppeer** {**address** {*ipv4-address* | **ipv6***ipv6-addressipv6-prefix-length*} | **hostname***fqdn-hostname*} 例： `Router(config)# crypto isakmp peer address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	IPsec ピアによるトンネル属性の IKE クエリーをイネーブルにします。
ステップ 4	**setaggressive-modeclient-endpoint**{*client-endpoint* | **ipv6***ipv6-address*} 例： `Router(config-isakmp-peer)# set aggressive mode client-endpoint ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	リモート ピアの IPv6 アドレスを定義します。このアドレスは、アグレッシブ モードのネゴシエーションで使用されます。通常、リモート ピアのアドレスはクライアント側のエンドポイント アドレスです。
ステップ 5	**end** 例： `Router(config-isakmp-peer)# end`	crypto ISAKMP ピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec トランスフォーム セットおよび IPsec プロファイルの定義

このタスクを実行して、IPsec トランスフォーム セットを定義します。トランスフォーム セットは、IPsec ルータに受け入れられるセキュリティ プロトコルとアルゴリズムの組み合わせです。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoipsectransform-set***transform-set-nametransform1* [*transform2*] [*transform3*] [*transform4*]
4. **cryptoipsecprofile***name*
5. **settransform-set***transform-set-name* [*transform-set-name2...transform-set-name6*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoipsectransform-set***transform-set-nametransform1* [*transform2*] [*transform3*] [*transform4*] 例： `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	トランスフォーム セットを定義し、ルータを暗号化トランスフォーム コンフィギュレーション モードにします。
ステップ 4	**cryptoipsecprofile***name* 例： `Router(config)# crypto ipsec profile profile0`	2 つの IPsec ルータ間における IPsec 暗号化のために使用される IPsec パラメータを定義します。
ステップ 5	**settransform-set***transform-set-name* [*transform-set-name2...transform-set-name6* 例： `Router (config-crypto-transform)# set-transform-set myset0`	クリプトマップ エントリで使用可能なトランスフォーム セットを指定します。

IPv6 での ISAKMP プロファイルの定義

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cryptoisakmpprofile***profile-name* [**accounting***aaalist*
4. **self-identity** {**address** | **addressipv6**] | **fqdn** | **user-fqdn***user-fqdn*}
5. **matchidentity** {**group***group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6***ipv6-address*} | **host***host-name* | **hostdomain***domain-name* | **user***user-fqdn* | **userdomain***domain-name*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoisakmpprofile***profile-name* [**accounting***aaalist* 例： `Router(config)# crypto isakmp profile profile1`	ISAKMP プロファイルを定義し、IPsec ユーザ セッションを監査します。
ステップ 4	**self-identity** {**address** | **addressipv6**] | **fqdn** | **user-fqdn***user-fqdn*} 例： `Router(config-isakmp-profile)# self-identity address ipv6`	ローカル IKE がリモート ピアに対して IKE 自身を識別させるために使用する ID を定義します。
ステップ 5	**matchidentity** {**group***group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6***ipv6-address*} | **host***host-name* | **hostdomain***domain-name* | **user***user-fqdn* | **userdomain***domain-name*}	ISAKMP プロファイルでリモート ピアの ID を照合します。

	コマンドまたはアクション	目的
	例： `Router(config-isakmp-profile)# match identity address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	
ステップ 6	**end** 例： `Router(config-isakmp-profile)# end`	ISAKMP プロファイル コンフィギュレーション モードを終了し、特権 sEXEC モードに戻ります。

IPv6 IPsec VTI の設定

はじめる前に

ipv6unicast-routing コマンドを使用して、IPv6 ユニキャスト ルーティングを有効化します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6unicast-routing**
4. **interfacetunnel***tunnel-number*
5. **ipv6address***ipv6-address/prefix*
6. **ipv6enable**
7. **tunnelsource** {*ip-address* | *ipv6-address* | *interface-typeinterface-number*}
8. **tunneldestination** {*host-name* | *ip-address* | *ipv6-address*}
9. **tunnelmode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gremultipoint** | **greipv6** | **ipip** [**decapsulate-any**] | **ipsecipv4** | **iptalk** | **ipv6** | **ipsecipv6** | **mpls** | **nos** | **rbscp**}
10. **tunnelprotectionipsecprofile***name* [**shared**]
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト ルーティングをイネーブルにします。設定するインターフェイス トンネルの数に関係なく、IPv6ユニキャストルーティングを有効化する必要があるのは 1 回だけです。
ステップ 4	**interfacetunnel***tunnel-number* 例： `Router(config)# interface tunnel 0`	トンネルインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ipv6address***ipv6-address/prefix* 例： `Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64`	IPv6 トラフィックをこのトンネルにルーティングできるように、このトンネル インターフェイスに対する IPv6 アドレスを指定します。
ステップ 6	**ipv6enable** 例： `Router(config-if)# ipv6 enable`	このトンネルインターフェイスに対して IPv6 をイネーブルにします。
ステップ 7	**tunnelsource** {*ip-address* | *ipv6-address* | *interface-typeinterface-number*} 例： `Router(config-if)# tunnel source ethernet0`	トンネルインターフェイスの送信元アドレスを設定します。
ステップ 8	**tunneldestination** {*host-name* | *ip-address* | *ipv6-address*} 例： `Router(config-if)# tunnel destination 2001:DB8:1111:2222::1`	トンネル インターフェイスの宛先を指定します。
ステップ 9	**tunnelmode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gremultipoint** | **greipv6** | **ipip** [**decapsulate-any**] | **ipsecipv4** | **iptalk** | **ipv6** | **ipsecipv6** | **mpls** | **nos** | **rbscp**}	トンネルインターフェイスのカプセル化モードを設定します。IPsec では、**ipsecipv6** キーワードだけがサポートされています。

	コマンドまたはアクション	目的
	例： `Router(config-if)# tunnel mode ipsec ipv6`	
ステップ 10	**tunnelprotectionipsecprofile***name* [**shared**] 例： `Router(config-if)# tunnel protection ipsec profile profile1`	トンネル インターフェイスを IPsec プロファイルに関連付けます。IPv6 では、**shared** キーワードはサポートされていません。
ステップ 11	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec トンネル モード設定の確認

手順の概要

1. **showadjacency** [**summary** [*interface-typeinterface-number*]] | [**prefix**] [**interface***interface-number*] [**connectionid***id*] [**link** {**ipv4**| **ipv6** | **mpls**}] [**detail**]
2. **showcryptoengine** {**accelerator** | **brief** | **configuration** | **connections** [**active** | **dh** | **dropped-packet** | **show**] | **qos**}
3. **showcryptoipsecsa** [**ipv6**] [*interface-typeinterface-number*] [**detailed**]
4. **showcryptoisakmppeer** [**config** | **detail**]
5. **showcryptoisakmppolicy**
6. **showcryptoisakmpprofile** [**tag***profilename* | **vrf***vrfname*]
7. **showcryptomap** [**interface***interface* | **tag***map-name*]
8. **showcryptosession** [**detail**] | [**local***ip-address* [**port***local-port*] | [**remote***ip-address*[**port***remote-port*]] | **detail**] | **fvfr***vrf-name*| **ivrf***vrf-name*]
9. **showcryptosocket**
10. **showipv6access-list** [*access-list-name*]
11. **showipv6cef** [*ipv6-prefix*/*prefix-length*] | [*interface-typeinterface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]]
12. **showinterface***typenumber***stats**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showadjacency** [**summary** [*interface-typeinterface-number*]] | [**prefix**] [**interface***interface-number*] [**connectionid***id*] [**link** {**ipv4**| **ipv6** | **mpls**}] [**detail**] 例： `Router# show adjacency detail`	シスコ エクスプレス フォワーディングの隣接関係テーブルまたはハードウェア レイヤ 3 スイッチングの隣接関係テーブルに関する情報を表示します。
ステップ 2	**showcryptoengine** {**accelerator** | **brief** | **configuration** | **connections** [**active** | **dh** | **dropped-packet** | **show**] | **qos**} 例： `Router# show crypto engine connection active`	暗号化エンジンの設定情報の要約を表示します。
ステップ 3	**showcryptoipsecsa** [**ipv6**] [*interface-typeinterface-number*] [**detailed**] 例： `Router# show crypto ipsec sa ipv6`	IPv6 で現在の SA によって使用されている設定を表示します。
ステップ 4	**showcryptoisakmppeer** [**config** | **detail**] 例： `Router# show crypto isakmp peer detail`	ピアの説明を表示します。
ステップ 5	**showcryptoisakmppolicy** 例： `Router# show crypto isakmp policy`	各 IKE ポリシーのパラメータを表示します。
ステップ 6	**showcryptoisakmpprofile** [**tag***profilename* | **vrf***vrfname*] 例： `Router# show crypto isakmp profile`	ルータに定義されている ISAKMP プロファイルをすべてリストします。
ステップ 7	**showcryptomap** [**interface***interface* | **tag***map-name*] 例： `Router# show crypto map`	クリプト マップの設定内容を表示します。 このコマンド出力で表示されるクリプト マップは、ダイナミックに生成されます。ユーザはクリプト マップを設定する必要はありません。

	コマンドまたはアクション	目的
ステップ 8	**showcryptosession** [**detail**] | [**local***ip-address* [**port***local-port*] | [**remote***ip-address*[**port***remote-port*]] | **detail**] | **fvfr***vrf-name*| **ivrf***vrf-name*] 例： `Router# show crypto session`	アクティブな暗号セッションのステータス情報を表示します。 IPv6 では、**fvfr** キーワード、**ivrf** キーワード、または *vrf-name* 引数はサポートされていません。
ステップ 9	**showcryptosocket** 例： `Router# show crypto socket`	暗号ソケットのリストを表示します。
ステップ 10	**showipv6access-list** [*access-list-name*] 例： `Router# show ipv6 access-list`	現在のすべての IPv6 アクセス リストの内容を表示します。
ステップ 11	**showipv6cef** [*ipv6-prefix*/*prefix-length*] | [*interface-typeinterface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]] 例： `Router# show ipv6 cef`	IPv6 転送情報ベース（FIB）のエントリを表示します。
ステップ 12	**showinterface***typenumber***stats** 例： `Router# show interface fddi 3/0/0 stats`	プロセス スイッチング、ファースト スイッチング、および分散スイッチングされたパケットの数を表示します。

IPsec for IPv6 の設定と動作のトラブルシューティング

手順の概要

1. イネーブル化
2. **debugcryptoipsec**
3. **debugcryptoenginepacket** [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugcryptoipsec** 例： `Router# debug crypto ipsec`	IPsec ネットワーク イベントを表示します。
ステップ 3	**debugcryptoenginepacket** [**detail**] 例： `Router# debug crypto engine packet`	IPv6 パケットの内容を表示します。 **注意** 複数のパケットが暗号化される場合、このコマンドを使用すると、システムのフラッディングが発生し、CPU 使用率が高くなる可能性があります。

IPv6 仮想トンネル インターフェイスの設定例

例：サイト間 IPv6 IPsec 保護用の VTI の設定

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
!
crypto isakmp key myPreshareKey0 address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128
crypto isakmp keepalive 30 30
!
crypto ipsec transform-set Trans1 ah-sha-hmac esp-aes
!
crypto ipsec profile profile0
  set transform-set Trans1
!
ipv6 cef
!
interface Tunnel0
  ipv6 address 3FFE:1001::/64 eui-64
  ipv6 enable
  ipv6 cef
  tunnel source Ethernet2/0
  tunnel destination 3FFE:2002::A8BB:CCFF:FE01:2C02
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile profile0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	『Cisco IOS Security Command Reference』
QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』
重み付け均等化キューイング	「Configuring Weighted Fair Queueing」機能モジュール

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

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

IPv6 仮想トンネル インターフェイスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *10* : *IPv6* 仮想トンネル インターフェイスの機能情報

機能名	リリース	機能情報
IPv6 仮想トンネル インターフェイス	Cisco IOS XE Release 2.4	IPsecは、インターネットなどの保護されていないネットワーク上の機密情報の送信にセキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。 次のコマンドが導入または変更されました。**authentication**（**IKE ポリシー**）、**crypto ipsec profile**、**crypto isakmp key**、**crypto isakmp peer**、**crypto isakmp policy**、**crypto isakmp profile**、**crypto keyring**、**debug crypto ipv6 ipsec**、**encryption**（**IKE ポリシー**）、**group**（**IKE ポリシー**）、**hash**（**IKE ポリシー**）、**lifetime**（**IKE ポリシー**）、**match identity**、**pre-shared-key**、**self-identity**、**set aggressive-mode client-endpoint**、**set transform-set**、**show adjacency**、**show crypto engine**、**show crypto ipsec sa**、**show crypto isakmp peers**、**show crypto isakmp policy**、**show crypto isakmp profile**、**show crypto map**、**show crypto session**、**show crypto socket**、**show ipv6 access-list**、**show ipv6 cef**、**tunnel destination**、**tunnel mode**、**tunnel source**

索 引

I

Invalid Security Parameter Index Recovery 22, 24, 34
その他の参考資料 34
確認 24
制約事項 22
前提条件 22
IP マルチキャスト ルーティング 105
MDS 105
パケット統計情報, 表示 105
IPSec 94
IPSec Dead Peer Detection 定期メッセージ オプション 38, 49
その他の参考資料 49
制約事項 38
前提条件 38
IPsec アンチ リプレイ ウィンドウ 7, 11
拡張と無効化 7, 11
設定例 7
IPsec トンネルを使用する DF ビット オーバーライド機能 68, 71
その他の関連資料 71
前提条件 68
68