RFC 430x IPsec サポート

RFC 430x IPsec サポートには、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装する機能（RFC 430x IPsec サポート フェーズ 1 およびフェーズ 2）が含まれます。

RFC 430x IPsec サポートに関する情報

RFC 430x IPsec サポート フェーズ 1

RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装します。

RFC 4301 は IPsec に準拠したシステムの基本アーキテクチャを規定しています。RFC 4301 には、IPv4 と IPv6 の両方の環境で、IP レイヤのトラフィックに一連のセキュリティ サービスを提供する方法が記載されています。RFC 430x IPsec サポート フェーズ 1 機能は、Cisco IOS ソフトウェア上の次の RFC 4301 実装をサポートします。

- **Security association (SA) lifetime**：IPSec とインターネット キー エクスチェンジ（IKE）またはインターネット キー エクスチェンジ バージョン 2（IKEv2）間のセキュリティ アソシエーションのライフタイムは認証証明書のライフタイムを超えないようにする必要があります。
- **OPAQUE selectors**：OPAQUE は、対応するセレクタフィールドが検証に使用できないことを示します。IKEv2 が OPAQUE セレクタに遭遇すると、IKEv2 はスキップして、OPAQUE セレクタを処理せず、ポリシー検証のために次のセレクタに移動します。
- **Explicit Congestion Notification (ECN) support**：ECN は、IPsec パケットの復号時に伝播されるため、パケットの送信元と宛先がネットワーク内で発生した輻輳を認識することが保証されます。

- **Fragment processing**：ピアは、同じトンネル内で初期フラグメントと非初期フラグメントを送信しないようにする必要があります。初期フラグメントと非初期フラグメントを伝送するためのトンネル モード SA と非初期フラグメント用のトンネル モード SA を分ける必要があります。IPsec ピアは、バイパス トラフィックに適合するために、パケットの破棄とステートフル フラグメント チェックをサポートする必要があります。
- **Do not fragment-(DF) bit processing**：DF ビット処理は、SA 単位で設定する必要があります。
- **Dummy packet generation support**：トラフィックが IPsec SA トンネル経由で流れている場合に IPsec SA 経由でダミーパケットを送信してパケットをカプセル化できる必要があります。

RFC 430x IPsec サポート フェーズ 2

RFC 430x IPsec サポート フェーズ 2 機能は、Cisco IOS ソフトウェア上の Internet Control Message Protocol（ICMP）パケットの暗号化と復号化の RFC 4301 実装をサポートします。

ICMP エラーが発生すると、ICMP エラー メッセージが送信されます。たとえば、ホストが到達不能の場合は、中間デバイスが ICMP 要求の発信元にホストが到達不能であることを示すメッセージを送信します。ICMP エラー メッセージが IPsec 暗号化ポリシーに届いた場合は、既存の SA と一致するように分類されない可能性があります。そのため、パケットは ICMP エラーメッセージ内のデータに基づいて分類されます。このデータには、元の ICMP メッセージの送信元アドレスと宛先アドレスが含まれています。SA が ICMP エラー メッセージ内のアドレスに基づいて検出された場合は、その SA が使用されます。SA が存在しない場合は、ポリシーで許可されていれば、SA が作成されます。復号化では、有効な SA が見つからない場合に、ICMP エラー メッセージ内のデータに基づいて復号化後チェックが実行されます。

ICMP エラーメッセージの暗号化と復号は、**show crypto ipsec sa** コマンドの出力に表示される暗号化カウンタと復号カウンタを通して確認できます。

RFC 430x IPsec サポートの設定方法

RFC 430x IPsec サポートのグローバル設定

このタスクは、RFC 4301 実装をグローバルに設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
4. **crypto ipsec security-association ecn** {**discard** | **propogate**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*} 例： `Device(config)# crypto ipsec security-association dummy seconds 5`	IPSec トラフィック フロー内のダミー パケットの生成と送信を可能にします。
ステップ 4	**crypto ipsec security-association ecn** {**discard** | **propogate**} 例： `Device(config)# crypto ipsec security-association ecn discard`	IPSec トラフィック フロー内の明示的輻輳通知（ECN）設定を可能にします。
ステップ 5	**exit** 例： `Device(config-crypto-map)# exit`	グローバル 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。

クリプト マップ単位の RFC 430x IPsec サポートの設定

このタスクは、RFC 4301 実装をクリプト マップ単位で設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set ipsec security-association dfbit** {**clear** | **copy** | **set**}
5. **set ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
6. **set ipsec security-association ecn** {**discard** | **propogate**}
7. **end**
8. **show crypto map ipsec sa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **ipsec-isakmp** 例： `Device(config)# crypto map cmap 1 ipsec-isakmp`	作成または変更するクリプト マップ エントリを指定して、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	**set ipsec security-association dfbit** {**clear** | **copy** | **set**} 例： `Device(config-crypto-map)# set ipsec security-association dfbit set`	クリプトマップ内の IPSec トラフィック フローのセキュリティ アソシエーション（SA）単位の Do not Fragment（DF）ビット処理を有効にします。
ステップ 5	**set ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*} 例： `Device(config-crypto-map)# set ipsec security-association dummy seconds 5`	クリプトマップ内の IPSec トラフィック フロー用のダミー パケットの生成と送信を有効にします。
ステップ 6	**set ipsec security-association ecn** {**discard** | **propogate**} 例： `Device(config-crypto-map)# set ipsec security-association ecn propogate`	クリプトマップ内の IPSec トラフィック フロー用の SA 単位の明示的輻輳通知（ECN）設定を有効にします。
ステップ 7	**end** 例： `Device(config-crypto-map)# end`	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show crypto map ipsec sa** 例： `Device# show crypto map ipsec sa`	IPsec SA によって使用される設定を表示します。

例

次に、**show crypto map ipsec sa** コマンドの出力例を示します。

```
Device# show crypto map ipsec sa

interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::32F7:DFF:FE54:7FD1
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (3FFE:2002::32F7:DFF:FE54:7FD1/128/47/0)
remote ident (addr/mask/prot/port): (3FFE:2002::C671:FEFF:FE88:EB82/128/47/0)
current_peer 3FFE:2002::C671:FEFF:FE88:EB82 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
#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
#send dummy packets 852600, #recv dummy packets 424905

local crypto endpt.: 3FFE:2002::32F7:DFF:FE54:7FD1,
remote crypto endpt.: 3FFE:2002::C671:FEFF:FE88:EB82
plaintext mtu 1430, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/0/1
current outbound spi: 0xE963D1EC(3915633132)
PFS (Y/N): N, DH group: none
Dummy packet: Initializing

inbound esp sas:
spi: 0xF4E01B9A(4108327834)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2053, flow_id: ESG:53, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xE963D1EC(3915633132)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2054, flow_id: ESG:54, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

RFC 430x IPsec サポートの設定例

例：RFC 430x IPsec サポートのグローバル設定

次に、RFC 430x IPsec サポートをグローバルに設定する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# crypto ipsec security-association dummy seconds 15
Device(config)# crypto ipsec security-association ecn propogate
Device(config-crypto-map)# exit
```

例：クリプト マップ単位の RFC 430x IPsec サポートの設定

次に、RFC 430x IPsec サポートをクリプト マップ単位で設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto map cmap 1 ipsec-isakmp
Device(config-crypto-map)# set security-association copy
Device(config-crypto-map)# set security-association dummy seconds 15
Device(config-crypto-map)# set security-association ecn propogate
Device(config-crypto-map)# end
Device# show crypto map ipsec sa

interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::32F7:DFF:FE54:7FD1
protected vrf: (none)
local ident (addr/mask/prot/port): (3FFE:2002::32F7:DFF:FE54:7FD1/128/47/0)
remote ident (addr/mask/prot/port): (3FFE:2002::C671:FEFF:FE88:EB82/128/47/0)
current_peer 3FFE:2002::C671:FEFF:FE88:EB82 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
#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
#send dummy packets 852600, #recv dummy packets 424905

local crypto endpt.: 3FFE:2002::32F7:DFF:FE54:7FD1,
remote crypto endpt.: 3FFE:2002::C671:FEFF:FE88:EB82
plaintext mtu 1430, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/0/1
current outbound spi: 0xE963D1EC(3915633132)
PFS (Y/N): N, DH group: none
Dummy packet: Initializing

inbound esp sas:
spi: 0xF4E01B9A(4108327834)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2053, flow_id: ESG:53, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xE963D1EC(3915633132)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2054, flow_id: ESG:54, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
```

```
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

RFC 430x IPsec サポートに関する追加のリファレンス

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』
IKEv2 の設定	
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
RFC 4301	『*Security Architecture for the Internet Protocol*』

シスコのテクニカル サポート

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

RFC 430x IPsec サポートに関する機能情報

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 : RFC430x IPsec* サポートに関する機能情報

機能名	リリース	機能情報
RFC430x IPsec サポート フェーズ 1		RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装します。 次のコマンドが導入または変更されました。 **crypto ipsec security-association dummy, crypto ipsec security-association ecn, set ipsec security-association dfbit, set ipsec security-association dummy, set ipsec security-association ecn, show crypto map ipsec sa.**
RFC430x IPsec サポート フェーズ 2		RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装します。 この機能に関して変更または更新されたコマンドはありません。

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