IPsec を使用した OSPFv3 認証サポートの設定

IPsec を使用した OSPFv3 認証サポートに関する情報

ここでは、IPsec および OSPFv3 仮想リンクを使用した OSPFv3 認証サポートについて説明します。

IPsec を使用した OSPFv3 認証サポートの概要

OSPFv3 パケットが変更されてデバイスに再送信されることにより、デバイスがシステム管理者にとって望ましくない動作をすることにならないように、OSPFv3 パケットを認証する必要があります。OSPFv3 は、IPsec セキュアソケットを使用して OSPFv3 パケットに認証を追加します。

OSPFv3 では、認証をイネーブルにするために IPsec を使用する必要があります。OSPFv3 で使用するために必要な IPsec は暗号イメージのみに含まれるため、認証を使用するには暗号イメージが必要です。

OSPFv3 では、認証フィールドが OSPFv3 パケット ヘッダーから削除されています。IPv6 で OSPFv3 を実行する場合、ルーティング変更の整合性、認証、および機密性を確保するために、OSPFv3 には IPv6 認証ヘッダーまたは IPv6 カプセル化セキュリティペイロード（ESP）ヘッダーが必要です。IPv6 認証ヘッダーおよび ESP 拡張ヘッダーを使用すると、OSPFv3 に認証および機密性を提供できます。

IPsec 認証ヘッダーを使用するには、**ipv6 ospf authentication** コマンドをイネーブルにする必要があります。IPsec ESP ヘッダーを使用するには、**ipv6 ospf encryption** コマンドをイネーブルにする必要があります。ESP ヘッダーは、単独で適用することも、認証ヘッダーとともに適用することもできます。ESP を使用した場合、暗号化と認証の両方が提供されます。セキュリティ サービスは、通信する 1 組のホスト、通信する 1 組のセキュリティ ゲートウェイ、またはセキュリティ ゲートウェイとホストの間に提供できます。

IPsec を設定するには、セキュリティポリシーを設定する必要があります。これは、Security Policy Index（SPI）とキーの組み合わせです（このキーはハッシュ値の作成および検証に使用されます）。OSPFv3 の IPsec は、インターフェイスまたは OSPFv3 エリアに対して設定できます。セキュリティを強化するには、IPsec を設定する各インターフェイスで異なるポリシーを設定する必要があります。OSPFv3 エリアに対して IPsec を設定した場合、ポリシーはそのエリア内のすべてのインターフェイス（IPsec が直接設定されているインターフェイスを除く）に適用されます。OSPFv3 に対して IPsec を設定すると、IPsec は見えなくなります。

アプリケーションは、IPsecure ソケットを使用することで、セキュアソケットのオープン、リッスン、およびクローズが可能になり、トラフィックが保護されます。また、アプリケーションと Secure Socket Layer の間のバインディングにより、Secure Socket Layer は、接続のオープンやイベントのクローズなど、ソケットへの変更をアプリケーションに通知できます。IPsecure ソケットは、ソケットを識別できます。つまり、セキュリティを必要とするトラフィックを伝送するローカルおよびリモートのアドレス、マスク、ポート、およびプロトコルを識別できます。

各インターフェイスのセキュア ソケット ステートは、次のいずれかになります。

- NULL：エリアに対して認証が設定されていれば、インターフェイスに対してセキュア ソケットを作成しません。
- DOWN：インターフェイス（またはインターフェイスが含まれるエリア）に対して IPsec は設定されていますが、OSPFv3 がこのインターフェイスに対するセキュアソケットの作成を IPsec に要求していないか、またはエラー条件が存在します。

（注） DOWN 状態の間は、OSPFv3 はパケットを受け入れたり、送信したりすることはありません。

- GOING UP：OSPFv3 はセキュア ソケットを IPsec に要求し、IPsec からの CRYPTO_SS_SOCKET_UP メッセージを待っています。
- UP：OSPFv3 は IPsec から CRYPTO_SS_SOCKET_UP メッセージを受信しました。
- CLOSING：インターフェイスのセキュア ソケットはクローズされています。インターフェイスに対して新しいソケットがオープンされることがあります。この場合、現在のセキュア ソケットは DOWN ステートに移行します。オープンされない場合、インターフェイスは UNCONFIGURED となります。
- UNCONFIGURED：インターフェイス上に認証は設定されていません。

OSPFv3 仮想リンク

仮想リンクごとに、プライマリセキュリティ情報データブロックが作成されます。各インターフェイスでセキュア ソケットをオープンする必要があるため、トランジット エリア内のインターフェイスごとに、対応するセキュリティ情報データブロックが存在することになります。セキュアソケットステートは、インターフェイスのセキュリティ情報データブロック内に保持されます。プライマリセキュリティ情報データブロック内の**ステート**フィールドは、対応する仮想リンクに対してオープンされたすべてのセキュアソケットのステータスを示します。すべてのセキュアソケットが UP の場合、仮想リンクのセキュリティステートは UP に設定されます。

IPsec が設定された仮想リンク上を送信されるパケットは、事前に決定された送信元アドレスと宛先アドレスを使用する必要があります。エリアのデバイスのエリア内プレフィックス リンクステート アドバタイズメント（LSA）で見つかった最初のローカルエリアアドレスが、送信元アドレスとして使用されます。この送信元アドレスはエリアのデータ構造に保存されます。セキュアソケットがオープンされ、パケットが対応する仮想リンク経由で送信されるときにこの送信元アドレスが使用されます。送信元アドレスが選択されるまで、仮想リンクはポイントツーポイント ステートに移行しません。また、送信元アドレスまたは宛先アドレスが変更された場合は、以前のセキュア ソケットをクローズして、新しいセキュア ソケットをオープンする必要があります。

（注） 仮想リンクは、IPv4 アドレスファミリについてはサポートされません。

IPsec を使用した OSPFv3 認証サポートの設定方法

ここでは、インターフェイスで認証を定義する方法と、OSPFv3 エリアで認証を定義する方法について説明します。

インターフェイスでの認証の定義

インターフェイスで認証を定義するには、次の手順を実行します。

始める前に

インターフェイスで IPsec を設定する前に、そのインターフェイスで OSPFv3 を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	プロンプトが表示されたらパスワードを入力します。
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	**interface** *type number* 例： `Device(config)# interface ethernet 1/0/1`	インターフェイスを設定します。

ステップ 4	次のいずれかを選択します。
	• **ospfv3 authentication** {{ **ipsec spi** *spi* {**md5** | **sha1**}} | { *key-encryption-type key* } | **null**}
	• **ipv6 ospf authentication** {**null** | **ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] [*key*]}
	例：
	`Device(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27`
	または
	`Device(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`
		インターフェイスの認証タイプを指定します。

OSPFv3 エリア内の認証の定義

OSPFv3 エリア内で認証を定義するには、次の手順を実行します。

手順

	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。 プロンプトが表示されたらパスワードを入力します。
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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router ospf** *process-id* 例： `Device(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* 例： `Device(config-router)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	OSPFv3 エリア内の認証をイネーブルにします。

OSPFv3 IPSec ESP 暗号化および認証の設定方法

ここでは、インターフェイスで暗号化を定義する方法、OSPFv3 エリアで暗号化を定義する方法、および OSPFv3 エリアで仮想リンクの認証と暗号化を定義する方法について説明します。

インターフェイスでの暗号化の定義

インターフェイスで暗号化を定義するには、次の手順を実行します。

始める前に

インターフェイスで IPsec を設定する前に、そのインターフェイスで OSPFv3 を設定する必要があります。

手順

	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。 プロンプトが表示されたらパスワードを入力します。
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	**interface** *type number* 例： `Device(config)# interface ethernet 1/0/1`	インターフェイスを設定します。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを選択します。
	• **ospfv3 authentication** { **ipsec spi** *spi* **esp** *encryption-algorithm key-encryption-type key authentication-algorithm key-encryption-type key* | **null**}
	• **ipv6 ospf authentication** { **ipsec spi** *spi* **esp** {*encryption-algorithm* [*key-encryption-type*] *key* | **null**} *authentication-algorithm* [*key-encryption-type*] *key*] | **null**}
	例：
	`Device(config-if)# ospfv3 encryption ipsec spi 1001 esp null md5 0 275761340947681324733020312097 27`
	または
	`Device(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D`
		インターフェイスに暗号化タイプを指定します。

OSPFv3 エリア内の暗号化の定義

OSPFv3 エリアで暗号化を定義するには、次の手順を実行します。

手順

	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。 プロンプトが表示されたらパスワードを入力します。
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	**ipv6 router ospf** *process-id* 例： `Device(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **encryption ipsec spi** *spi* **esp** {*encryption-algorithm* [*key-encryption-type*] *key* | **null**} *authentication-algorithm* [*key-encryption-type*] *key*	OSPFv3 エリア内の暗号化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： `Device(config-router)# area 1 encryption ipsec spi 500 esp null md5 1aaa2bbb3ccc4ddd5eee6fff7aaa8bbb`	

OSPFv3 エリア内の仮想リンクに対する認証および暗号化の定義

OSPFv3 エリア内の仮想リンクに対する認証および暗号化を定義するには、次の手順を実行します。

手順

	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。 プロンプトが表示されたらパスワードを入力します。
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	**ipv6 router ospf** *process-id* 例： `Device(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* 例： `Device(config-router)# area 1 virtual-link 10.0.0.1 authentication ipsec spi 940 md5 1234567890ABCDEF1234567890ABCDEF`	OSPFv3 エリア内の仮想リンクに対して認証をイネーブルにします。
ステップ 5	**area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi* **esp** {*encryption-algorithm* [*key-encryption-type*] *key* | **null**} *authentication-algorithm* [*key-encryption-type*] *key* 例： `Device(config-router)# area 1 virtual-link 10.1.0.1 hello-interval 2 dead-interval 10 encryption ipsec`	OSPFv3 エリア内の仮想リンクに対して暗号化をイネーブルにします。

	コマンドまたはアクション	目的
	spi 3944 esp null sha1 123456789A123456789B123456789C123456789D	

IPsec を使用した OSPFv3 認証サポートの設定例

ここでは、IPsec を使用した OSPFv3 認証サポートのさまざまな設定例を示します。

例：インターフェイスでの認証の定義

次に、イーサネット インターフェイス 1/0/1 で認証を定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Ethernet1/0/1
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 ospf 1 area 0
Device(config-if)# ipv6 ospf authentication ipsec spi 500 md5
1234567890ABCDEF1234567890ABCDEF
Device(config-if)# exit
Device(config)# interface Ethernet1/0/1
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 ospf authentication null
Device(config-if)# ipv6 ospf 1 area 0
```

例：OSPFv3 エリア内の認証の定義

次に、OSPFv3 エリア 0 で認証を定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 router ospf 1
Device(config-router)# router-id 10.11.11.1
Device(config-router)# area 0 authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

OSPFv3 IPSec ESP 暗号化および認証の設定例

ここでは、OSPFv3 IPsec ESP 暗号化および認証を確認する例を示します。

例：OSPFv3 エリアでの暗号化の確認

次に、**show ipv6 ospf interface** コマンドの出力例を示します。

```
Device> enable
Device# show ipv6 ospf interface

Ethernet1/0/1 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

IPsec を使用した OSPFv3 認証サポートの機能履歴と機能情報

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。

表 *1 : IPsec* を使用した *OSPFv3* 認証サポートの機能履歴

機能名	リリース	機能情報
IPsec を使用した OSPFv3 認証サポート	Cisco IOS XE Fuji 16.8.1a	OSPFv3 は、IPsec セキュアソケットを使用して OSPFv3 パケットに認証を追加します。