IPSec ポリシーの管理

- IPsec ポリシーの概要 （1 ページ）
- IPsec ポリシーの設定 （2 ページ）
- IPsec 証明書の確認, on page 3
- IPSec ポリシーの管理 （3 ページ）

IPsec ポリシーの概要

IPsec は、暗号セキュリティ サービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。IPsec ポリシーが IPsec セキュリティ サービスの設定に使用されます。このポリシーは、ネットワーク上のほとんどのトラフィック タイプにさまざまなレベルの保護を提供します。コンピュータ、部門（OU）、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

IPsec ポリシーの設定

（注）
- システムアップグレード中に IPsec ポリシーに対して行った変更は無効となるので、アップグレード中は IPsec ポリシー を修正または作成しないでください。
- IPsec には双方向プロビジョニングが必要です（ホストまたはゲートウェイごとに 1 ピア）。
- 一方の IPsec ポリシー プロトコルが 「ANY」、もう一方の IPsec ポリシー プロトコルが 「UDP」 または 「TCP」 に設定されている 2 つの Unified Communications Manager ノードに IPsec ポリシーをプロビジョニングする場合、「ANY」 プロトコルを使用するノードでの検証で検出漏れが発生する可能性があります。
- IPsec はシステムのパフォーマンスに影響します（特に暗号化した場合）。
- IPsec ポリシーが現在のバージョンまたはアップグレードされたバージョンで構成されていますが、基本バージョンで構成されていない場合は、このバージョンを基本バージョンに切り替えるときに、IPsec ポリシーを削除するか無効にしてください。これは、いずれかのノードのみで IPsec ポリシーが構成され、両方のバージョンをスイッチバックするまで、他ノードには、 IPsec ポリシーが構成されないためです。そうしないと、接続の問題が発生します。
- Unified CM ノードの再起動後、IPsec 接続が起動していない場合は、**utils ipsec restart** コマンドを使用して IPsec サービスを再起動し、IPsec 接続を正常に確立してください。この回避策は、ネットワーク接続が確立される前に IPsec サービスを再起動する際の問題を軽減するために行います。

手順

ステップ 1 Cisco Unified OS の管理から **[セキュリティ（Security）] > [IPSec の設定（IPSec Configuration）]** の順に選択します。

ステップ 2 **[新規追加（Add New）]** をクリックします。

ステップ 3 [IPSEC ポリシーの設定（IPSEC Policy Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 （任意） IPsec を検証するには、**[サービス（Services）] > [Ping]** の順に選択し、[IPsec の検証（Validate IPsec）] チェックボックスをオンにして、[Ping] をクリックします。

IPsec 証明書の確認

次の手順を使用して、IPsec 証明書を確認します。

Procedure

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から **[セキュリティ（Security）]** > **[管理証明書（Management Certificate）]**を選択します。

ステップ 2 検索情報を指定し、[検索（Find）] をクリックします。

ステップ 3 IPsec 証明書を検索します（パブリッシャノードとサブスクライバノードに個別にログインします）。

Note 通常、サブスクライバノードの IPsec 証明書はパブリッシャノードで表示できません。ただし、パブリッシャノードの IPsec 証明書は、IM&P ノードのサブスクライバノードで表示できます。

IPsec 接続を有効にするには、一方のノードからの CA 署名付き IPsec 証明書を、もう一方のノードの **IPsec-Trust** 証明書として使用する必要があります。

新しい証明書を **IPsec-Trust** にアップロードする前に、**IPsec-Trust** で同じ共通名を持つ以前の証明書を削除する必要があります。

IPSec ポリシーの管理

システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

⚠

注意 ホスト名、ドメイン、またはIPアドレスを変更するために既存のIPSec証明書に変更を加える際、証明書名を変更する場合は、IPSec ポリシーを削除して作り直す必要があります。証明書名を変更しない場合は、リモート ノードの作り直した証明書をインポートした後に、IPSec ポリシーを無効にして有効にする必要があります。

手順

ステップ 1 Cisco Unified OS の管理から **[セキュリティ（Security）]** > **[IPSec の設定（IPSec Configuration）]** の順に選択します。

ステップ 2 ポリシーを表示、イネーブル、またはディセーブルにするには、次の手順を実行します。

a) ポリシー名をクリックします。

b) ポリシーを有効または無効にするには、[ポリシーの有効化（Enable Policy）] チェックボックスをオンまたはオフにします。
c) [保存（Save）] をクリックします。
d) ポリシーを無効にする場合、無効化の変更を有効にするには、**utils ipsec restart** コマンドを実行する必要があります。

ステップ 3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a) 削除するポリシーの横にあるチェックボックスをオンにします。

[すべてを選択（Select All）] をクリックするとすべてのポリシーを選択でき、[すべてをクリア（Clear All）] を選択するとすべてのチェックボックスをクリアできます。

b) [選択項目の削除（Delete Selected）] をクリックします。

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。