ネットワーク分離ユーティリティを使用した IPSec

IPsec

インターネット プロトコル セキュリティ（IPSec）は、Microsoft、Cisco およびその他の多くのインターネット技術特別調査委員会（IETF）の貢献企業によって共同で開発されたセキュリティ標準です。エンドポイントやゲートウェイなど、任意の2つのノード間で整合性（認証）と暗号化を提供します。IPSec は、ネットワークのレイヤ 3 で動作するため、アプリケーションに依存しません。IPSec は、アプリケーションに依存しないアプリケーションノード間でセキュリティを提供する Unified ICM のような大規模で分散されたアプリケーションに役立ちます。

詳細については、https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configurationを参照してください。

手動導入またはネットワーク分離ユーティリティ

ネットワーク分離ユーティリティは、IPSec を使用して Unified ICM/Unified CCE 環境を保護するための作業の大半を自動化します。ネットワーク分離ユーティリティは、Unified ICM/Unified

CCE サーバとの間でネットワークトラフィック全体を保護する事前設定済みの IPSec ポリシーを導入します。ネットワーク接続は、同じポリシーを共有するサーバ、または例外として明示的にリストされているサーバにのみ制限されます。

選択した通信パス間でのみネットワークトラフィックを保護する場合は、ネットワーク分離ユーティリティを使用しません。

関連トピック

ネットワーク分離ユーティリティを使用した IPSec

シスコのネットワーク分離ユーティリティ

シスコネットワーク分離ユーティリティは、Windows IPSec 機能を使用して、Unified ICM デバイスをネットワークの他の部分から分離します。Unified ICM デバイスの例には、ルータ、ロガー、および周辺ゲートウェイデバイスが含まれます。このユーティリティは、ネットワーク分離 IPSec ポリシーを作成し、Unified ICM デバイスを信頼済みとして設定し、信頼済みデバイス間のすべてのトラフィックを認証およびオプションで暗号化します。信頼済みデバイス間のトラフィックは、設定を追加することなく通常通り継続して流れます。境界デバイス間のトラフィックとして分類されていない限り、信頼済みデバイス以外のデバイス間のすべてのトラフィックは拒否されます。

境界デバイスは、信頼済みデバイスへのアクセスが許可されている IPSec ポリシーを持つデバイスです。通常、これらのデバイスには、ドメインコントローラ、Unified CM、デフォルト ゲートウェイ デバイス、有用性デバイス、リモート アクセス コンピュータが含まれます。

信頼済みデバイスごとに、境界デバイスのリストが用意されています。個別の IP アドレスまたはサブネットまたはポートが、境界デバイスを定義します。

ネットワーク分離ポリシーでは、整合性と暗号化に IPsec ESP（カプセル化セキュリティ ペイロード）プロトコルが使用されます。導入される暗号スイートは次のとおりです。

- IP トラフィックセキュリティ：
  - 整合性アルゴリズム：SHA1
  - 暗号化アルゴリズム：3DES
- キー交換セキュリティ：
  - 整合性アルゴリズム：SHA1
  - 暗号化アルゴリズム：3DES（オプション）
  - Diffie-Hellman グループ：高（2048 ビットキー）

ネットワーク分離ユーティリティ情報

次のセクションでは、ネットワーク分離ユーティリティの設計と動作について説明します。

IPSec 用語

次のリストには、IPSec の基本用語の定義が含まれます。

ポリシー

IPSec ポリシーは、IPSec の動作を決定する 1 つ以上のルールの集大集です。Windows Server では複数のポリシーを作成できますが、一度に割り当てられるポリシー（アクティブ）は 1 つのみです。

ルール

各ルールは、FilterList、FilterAction、認証方式、TunnelSetting、および ConnectionType の各ルールで構成されます。

フィルタリスト

フィルタリストは、送信元および宛先の IP アドレス、プロトコル、およびポートに基づいて IP パケットと一致するフィルタのセットです。

フィルタ アクション

フィルタアクションは、フィルタリストで識別され、データ送信のセキュリティ要件を定義します。

認証方式

認証方式では、関連付けられたルールを適用する通信で ID を検証する方法の要件を定義します。

Microsoft Windows IPSec に関する用語の詳細については、次を参照してください。

https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configuration.

ネットワーク分離ユーティリティプロセス

信頼済みデバイスごとにネットワーク分離ユーティリティを個別に実行します。境界デバイスでこのユーティリティを実行**しないでください**。

境界デバイス間のトラフィックを許可するには、信頼済みデバイスごとに [境界デバイス（Boundary Device）] リストを手動で設定します。

デバイスへのネットワーク分離 IPSec ポリシーの導入後、そのデバイスは [信頼済み（Trusted）] に設定されます。トラフィックは、設定を追加することなく、そのデバイスと他の信頼済みデバイスとの間で自由にフローします。

ネットワーク分離ユーティリティを実行すると、次の動作が実行されます。

1. そのコンピュータ上にすでに存在する IPSec ポリシーを削除します。この削除により競合が回避され、新しいポリシーがすべての Unified ICM デバイスと一致して導入が成功します。
2. Windows IPSec ポリシーストアに Cisco Unified Contact Center（ネットワーク分離）IPSec ポリシーを作成します。

3. ポリシーに対して次の 2 つのルールを作成します。

   1. **信頼済みデバイスのルール**

      このルールには、次の項目が含まれます。

      - **信頼済みデバイスのフィルタリスト**：すべてのトラフィック。すべてのトラフィックに一致する 1 つのフィルタ。
      - **信頼済みデバイスのフィルタアクション**：セキュリティが必要です。整合性アルゴリズム SHA1 を使用して認証し、必要に応じて暗号化アルゴリズム 3DES を使用して暗号化します。
      - **認証方法**：コンピュータ間の信頼を作成するために使用される認証方法は、事前共有キーです。

        事前共有キーは、二重引用符を除く一文字列の単語、数字、または文字を使用できます。このキーの最小長は 36 文字です。

   2. **境界デバイスルール**

      このルールには、次の項目が含まれます。

      - **境界デバイスフィルタリスト**：（デフォルトでは空）
      - **境界デバイスフィルタアクション**：IPSecポリシーなしでトラフィックを許可します。境界デバイスでは、信頼済みデバイスとの通信に IPSec が必要ではありません。

4. ネットワーク 分離ユーティリティは、Cisco Unified Contact Center の IPSec ポリシーのコピーをネットワーク分離ユーティリティフォルダ（`<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML`）にある XML ファイルに保存します。

   XML ファイルには、ポリシーの状態と境界デバイスのリストが格納されます。事前共有キーは保存されません。

5. ネットワーク分離ユーティリティは、`<SystemDrive>:\CiscoUtils\NetworkIsolation\Logs\CiscoICMNetworkIsolation.log` にあるログファイルに、すべてのコマンドとアクションを記録します。

   このユーティリティは、ログファイルのコピーを 1 つ保持し、すべてのコマンドとアクションを以前に作成したログに追加します。

トラフィックの暗号化とネットワーク分離ポリシー

ネットワーク分離ポリシーでは、同じ事前共有キーを持つコンピュータのみを操作できます。ネットワーク分離機能を使用すると、外部のハッカーは信頼できるコンピュータにアクセスできません。ただし、暗号化を有効にしない場合は、ハッカーはそのコンピュータからトラフィッ

クが行き来しているのを見ることができます。したがって、そのトラフィックを暗号化することを検討してください。

（注）

- 1 つの信頼済みデバイスに対するトラフィックは、単独では暗号化できません。すべての信頼済みデバイス上、またはデバイス上ではないトラフィックを暗号化します。1 つのコンピュータだけがトラフィックを暗号化している場合は、他の信頼済みデバイスのいずれもトラフィックを理解しません。
- 暗号化で IPSec が有効になっている場合は、暗号化オフロード NIC を使用します。そうすることで、暗号化ソフトウェアがパフォーマンスに影響を与えるのを防ぐことができます。

関連トピック

IPSec の概要
IPSec および NAT のサポート

ネットワーク分離機能の導入

次のセクションでは、展開プランの設計時に注意する必要がある問題について説明します。

関連トピック

境界デバイスと Unified CCE （9 ページ）
デバイスの双方向の通信 （8 ページ）
重要な導入のヒント （5 ページ）
導入例 （5 ページ）

重要な導入のヒント

境界デバイスの設定は不要です。すべての設定は信頼済みデバイスで行われます。ネットワーク分離ユーティリティは、信頼済みデバイスを他の信頼済みデバイスや境界デバイスとやり取りするために設定します。ネットワーク分離機能は、一度に 1 つのデバイスに適用されます。この機能により、適用後に他のデバイスとの通信が瞬時に制限されます。したがって、この機能を使用する前に、この機能の導入方法を慎重に計画しないと、ネットワークの動作を誤って停止する可能性があります。ネットワーク分離機能を実装する前に、導入計画を作成します。このため、この機能はメンテナンスウィンドウでのみ導入し、導入計画を作成する前に警告を確認してください。

関連トピック

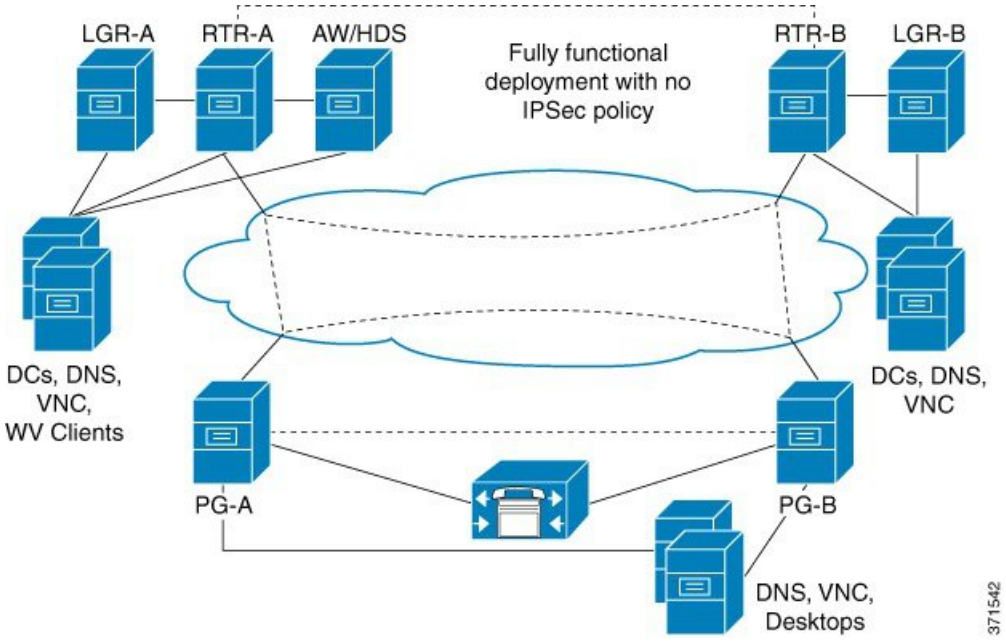
注意事項 （10 ページ）

導入例

導入例の 1 つを以下に示します。

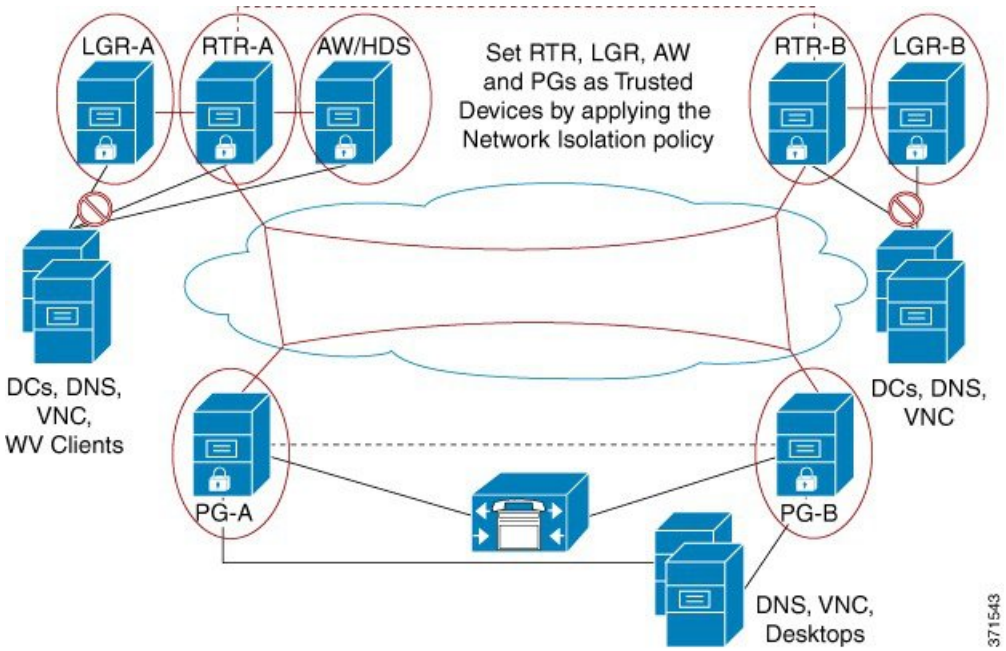
1. IPSec ポリシーを導入できる、完全に機能する Unified ICM または Unified CCE システムから開始します。

図 *1:* ユニファイド コンタクト センターのシステムの例



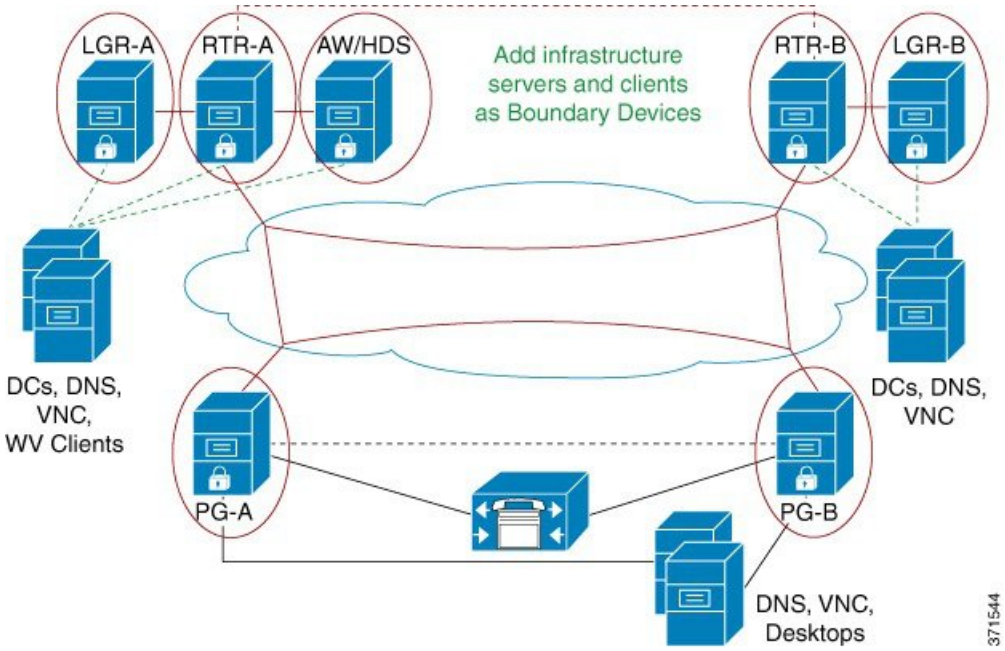
2. ネットワーク分離ユーティリティを CallRouter、ロガー、管理 & データサーバおよび PG に実行することで、それぞれを信頼済みデバイスとして設定します。

図 *2:* 例：信頼済みデバイスの追加



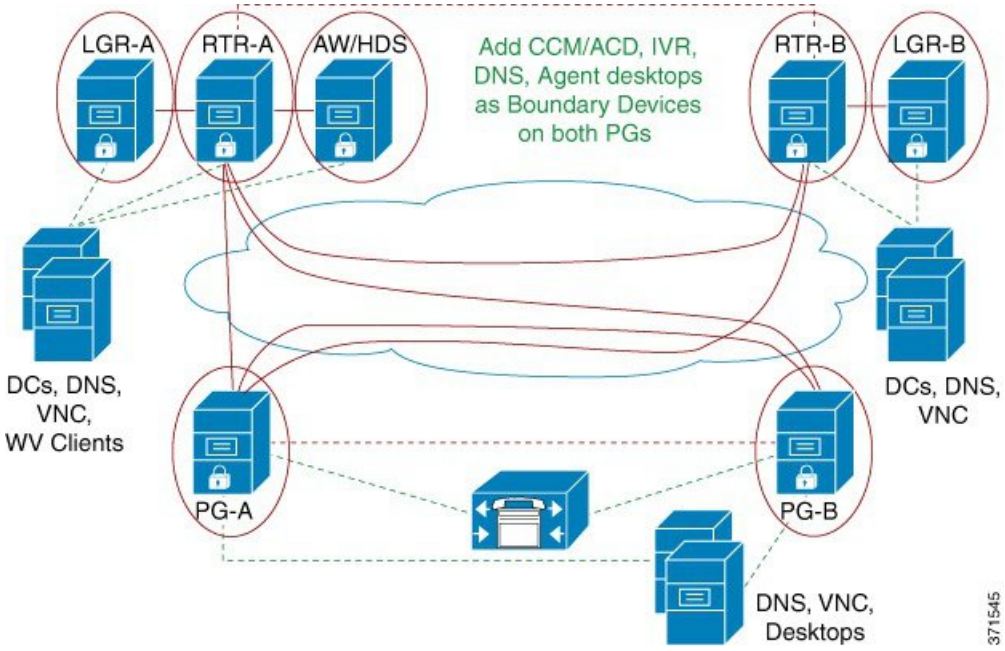
3. インフラストラクチャサーバとクライアントを境界デバイスとして追加します。

図 3：例：境界デバイスの追加



4. Unified Communications Manager または ACD サーバ、DNS、およびエージェントデスクトップを両方の PG に境界デバイスとして追加します。

図 4：例：*PG* への境界デバイスの追加



完了すると、すべてのユニファイド コンタクト センターの信頼済みデバイスが相互にのみ通信し、それぞれの境界デバイス（ドメインコントローラ、DNS、Unified Communications Managerなど）と通信します。外部からのネットワーク攻撃は、境界デバイスを介してルーティングされていない限り、信頼済みデバイスに到達できません。

デバイスの双方向の通信

この表は、Unified CCE 導入での 2 者間通信の要件を示します。対象のデバイスを信頼済みデバイスまたは境界デバイスとして設定できます。

Unified CCE コンポーネント	**対象デバイス**
CallRouter	CallRouter（冗長システムのもう一方の側）
	ロガー
	管理&データサーバ/履歴データベースサーバ
	NAM ルータ
	周辺機器ゲートウェイ（冗長システムの両側）
	アプリケーション ゲートウェイ
	データベースサーバー
	ネットワークゲートウェイ（Network Gateway）
ロガー	履歴データベースサーバ/管理&データサーバ
	CallRouter
	Campaign Manager
	ダイヤラ
Peripheral Gateway	マルチチャネル/マルチメディアサーバ
	CallRouter（冗長システムの両側）
	周辺機器ゲートウェイ（冗長システムのもう一方の側）
	Unified Communications Manager
	管理&データサーバレガシーの PIMS/スイッチ

Unified CCE コンポーネント	対象デバイス
管理&データサーバ/履歴データベースサーバ	マルチチャネル/マルチメディアサーバ
	ルータ
	Logger
	カスタム アプリケーション サーバ
	CON API クライアント
	インターネット スクリプト エディタ クライアント/Web スキリング
	サードパーティ クライアント/SQL パーティ
管理サーバ、リアルタイムおよび履歴データサーバ、および詳細データサーバ（AW-HDS-DDS）	マルチチャネル/マルチメディアサーバ
	ルータ
	Logger
	カスタム アプリケーション サーバ
	インターネット スクリプト エディタ クライアント/Web スキリング
	サードパーティ クライアント/SOL パーティ

境界デバイスと Unified CCE

この表は、Unified CCE 導入で通常必要な境界デバイスの一覧を示します。

境界デバイス	設定例
ドメインコントローラ：RTR、LGR、管理 & データサーバまたは HDS、PG	• 境界デバイス：ドメインコントローラの IP アドレス • トラフィックの方向：アウトバウンド • プロトコル；任意 • ポート：適用されない
DNS、WINS、デフォルトゲートウェイ	—

境界デバイス	設定例
リモートアクセスまたはリモート管理ソフトウェア：信頼済みのすべてのデバイス（VNC、pcAnywhere、リモートデスクトップ接続、SNMP）など	*VNC*： • 境界デバイス：任意のホスト • トラフィックの方向：インバウンド • [プロトコル（Protocol）]：TCP • ポート：5900
PG の Unified Communications Manager クラスタ	• 境界デバイス：特定の IP アドレス（またはサブネット） • トラフィックの方向：アウトバウンド • [プロトコル（Protocol）]：TCP • ポート：すべてのポート
[エージェントのデスクトップ（Agent Desktops）]	*Finesse* サーバ： • 境界デバイス：サブネット • トラフィックの方向：インバウンド • [プロトコル（Protocol）]：TCP • ポート：42028

注意事項

ポリシーがすべてのマシンに同時に適用されるよう、導入を慎重に計画します。そうでないと、誤ってデバイスを分離する場合があります。

注意点は次のとおりです。

-

重要 ポリシーをリモートで有効にすると、リモートアクセス用の境界デバイスリストにプロビジョニングが行なわれていない限り、リモートアクセスがブロックされます。リモートでポリシーを有効にする前に、リモートアクセス用の境界デバイスを追加します。

-

重要 境界デバイスとしてすべてのドメインコントローラを追加しないと、ドメインログインが失敗します。ドメインログインが失敗した場合は、Unified ICM サービスも開始に失敗するか、ログイン時間の遅延を確認できます。ドメインコントローラのこのリストには、Unified ICM がインストールされているすべてのドメインが含まれます。このリストには、Web セットアップツール、設定ユーザ、およびスーパーバイザが存在するすべてのドメインも含まれています。

- 境界デバイスとして新しいデバイスを追加するには、IPSec を使用せずにこの新しいデバイスにアクセスする必要があるすべての信頼済みデバイスのポリシーを変更する必要があります。
- すべての信頼済みデバイスで事前共有キーの変更を呼び出す必要があります。
- 1 つの信頼済みデバイスだけで暗号化を有効にした場合、ネットワークトラフィックが暗号化されているため、そのデバイスは他の信頼済みデバイスと通信できません。信頼済みデバイスのすべてで暗号化を有効または無効にします。
- Windows IPSec ポリシー MMC プラグインを使用して IPSec ポリシーを変更することはできません。ネットワーク分離ユーティリティは、ポリシーの独自のコピーを保持します。ネットワーク分離ユーティリティを実行すると、ユーティリティ以外（またはセキュリティウィザード）で行われた変更を無視して、ユーティリティは最後に保存された設定に戻ります。
- ネットワーク分離ユーティリティは、ネットワーク上で実行されるアプリケーションに干渉しません。ただし、ユーティリティはアプリケーションのメンテナンスウィンドウでのみ実行します。このユーティリティは、ネットワークセキュリティを設定するときに接続が中断される可能性があるからです。
- ネットワークがファイアウォールの背後にある場合は、次の方法でファイアウォールを設定します。
  - IP プロトコル番号として、ESP（カプセル化セキュリティプロトコル）である 50 を許可します。
  - IKE プロトコルに対して、ポート 500 で UDP の送信元と宛先のトラフィックを許可します。
- NAT プロトコルを使用している場合は、ファイアウォールを設定して、UDP-ESP のカプセル化用に UDP 送信元と宛先ポート 4500 でトラフィックを転送します。
- Web サーバポートなど、アプリケーションポートの使用法に加えた変更は、ポリシーにも反映する必要があります。
- Unified ICM またはユニファイドコンタクトセンターアプリケーションが設定され、動作を確認した後に、ネットワーク分離ポリシーを導入します。

- アプリケーションのコンタクトセンタースイート全体で使用されているポートのインベントリについては、次のドキュメントを参照してください。
  - *Cisco Unified Contact Center Enterprise Solutions* ポート使用状況ガイド https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html
  - https://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

ファイアウォールの構成を支援するため、このガイドにはエージェントデスクトップとサーバ間の通信、アプリケーション管理、およびレポート生成に使用されるプロトコルとポートが記載されています。また、イントラサーバ通信に使用されるポートのリストも記載されています。

バッチ導入

すべての信頼済みデバイスに共通の境界デバイスを追加する必要が生じた場合、導入の迅速化に役立つ次の XML ファイルを使用できます。

`<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML`

この XML ファイルには、1 つの信頼済みデバイスに対する境界デバイスのリストとポリシー状態が含まれています。このファイルを使用すると、他の信頼済みデバイス上でポリシーを複製できます。

たとえば、信頼済みデバイスとして PG を設定する場合は、最初に 1 つの Unified ICM PG の設定を完了できます。次に、その PG から他の Unified ICM PG に XML ファイルをコピーできます。その後、他の PG で分離ユーティリティ（またはセキュリティウィザード）を実行して、すべての PG 上で同じ境界デバイスのリストを作成します。

ネットワーク分離ユーティリティのコマンドラインシンタックス

ネットワーク分離ユーティリティは、コマンドラインまたは Unified Contact Center Security ウィザードから実行できます。

（注） 最初のポリシーの作成または変更には、セキュリティウィザードを使用します。コマンドラインを使用して、バッチ導入ができます。

コマンドラインからユーティリティを実行するには、ユーティリティがある C:\CiscoUtils\NetworkIsolation ディレクトリに移動し、そこから実行します。

C:\CiscoUtils\NetworkIsolation>

信頼済みデバイスでポリシーを有効にするためのコマンドラインシンタックスを次に示します。

```
cscript ICMNetworkIsolation.vbe <arguments>
```

（注） スクリプトを呼び出す場合は、**cscript** を使用する必要があります。

複数のフィルタを使用して、境界デバイスを追加できます。次の条件でフィルタリングできます。

- **IP アドレス**：個々の IP アドレス、またはデバイスのサブネット全体
- **動的に検出されたデバイス**：DNS、WINS、DHCP、デフォルトゲートウェイ

  Windows は、これらのデバイスの IP アドレスを動的に検出し、フィルタリストの更新を維持します。
- **トラフィックの方向**：インバウンドまたはアウトバウンド
- **プロトコル**：TCP、UDP、ICMP、または任意のプロトコル
- **ポート**（TCP または UDP が選択されている場合のみ）：特定のポートまたはすべてのポート

シンタックス内：

- 山カッコ <>= 必須
- 角カッコ [ ] = 任意
- パイプまたはバー | = バーの間のいずれかの項目

次の表に、コマンドのすべての使用に関するコマンドシンタックスを示します。

表 *1:* 各引数のネットワーク分離ユーティリティ コマンド シンタックス

引数名	構文と例	機能
HELP	cscript ICMNetworkIsolation.vbe /?	コマンドのシンタックスを表示します。
ENABLE POLICY	cscript ICMNetworkIsolation.vbe /enablePolicy <36+ characters PreSharedKey in double quotes> [/encrypt] （注） PresharedKey で使用する唯一の非対応文字は二重引用符です。その文字はキーの始めと終わりをマークします。キー内の他の任意の文字を入力できます。 次に例を示します。 `cscript ICMNetworkIsolation.vbe /enablePolicy 「myspecialpresharedkey123456789mnbvcx」`	新しいポリシーを作成するか、保存されているポリシー XML ファイルから既存のポリシーを有効にします。 必要に応じて、ネットワーク トラフィック データの暗号化を有効にします。 Windows IPSec ポリシーストアに新しいポリシーを作成し、XML ファイルにリストされているすべての境界デバイスを追加します。XML ファイルが存在しない場合、新しい XML ファイルが作成されます。/encrypt オプションは、XML ファイルで設定されている値を上書きします。
（注） 追加、削除、および削除の引数では、XML ファイルのバックアップを作成し、その機能を実行する前に xml.lastconfig という名前を付します。		

引数名	構文と例	機能
ADD BOUNDARY	cscript ICMNetworkIsolation.vbe /addBoundary DNS|WINS|DHCP|GATEWAY 次に例を示します。 `cscript ICMNetworkIsolation.vbe /addBoundary DNS` この例では、DNS サーバを境界デバイスリストに追加します。	指定されたデバイスの種類を、境界デバイスリストに追加します。 このタイプは、DNS、WINS、DHCP、またはGATEWAYとして指定できます。 このユーティリティは、DNS、WINS、DHCP、および GATEWAY をそれぞれドメインネームシステム（DNS）デバイス、Windows インターネット ネーム サービス（WINS）デバイス、Dynamic Host Configuration Protocol（DHCP）デバイス、デフォルトゲートウェイ（GATEWAY）デバイスとして認識します。 Windows オペレーティングシステムは、上記のタイプの各デバイスの IP アドレスの変更を動的に検出し、それに応じて境界フィルタリストを動的に更新します。
	cscript ICMNetworkIsolation.vbe /addAnyHostBoundary <Outbound|Inbound> <TCP|UDP> <PortNumber> 次に例を示します。 `cscript ICMNetworkIsolation.vbe /addAnyHostBoundary Inbound TCP 5900` この例では、すべてのマシンからの VNC アクセスを許可します。	次の基準に一致するデバイスのリストが、境界デバイスに追加されます。 • 指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。 • 指定されたプロトコルの 1 つ、Transmission Control Protocol（TCP）または User Datagram Protocol（UDP）。 • 指定されたポート。

引数名	構文と例	機能
	cscript ICMNetworkIsolation.vbe /addIPAddrBoundary <IP address> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] 次に例を示します。 `cscript ICMNetworkIsolation.vbe /addIPAddrBoundary 10.86.121.160 Outbound Any` この例では、指定されたIPアドレスを持つデバイスへのすべてのアウトバウンドトラフィックを許可します。	次の構成を持つデバイスのIPアドレスが、境界デバイスのリストに追加されます。 • （必須）指定された IP アドレス。 • （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。 • （必須）指定されたプロトコル（必須）：Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）、または任意のプロトコル。 • （任意）選択したプロトコルがTCPまたはUDPの場合、任意のポートまたは指定されたポート。
	cscript ICMNetworkIsolation.vbe /addSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber]	

引数名	構文と例	機能
		次の構成を持つサブネットを、境界デバイスリストに追加します。 • （必須）次に指定した範囲の開始 IP アドレス。 • （必須）指定されたサブネットマスク（アドレス空間内の論理的なアドレスの範囲）。 • （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。 • （必須）指定されたプロトコル、Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）、または任意のプロトコル。 • （任意）プロトコルとして TCP または UDP が選択された場合、任意のポートまたは指定されたポート。

引数名	構文と例	機能
REMOVE BOUNDARY	cscript ICMNetworkIsolation.vbe /removeBoundary DNS|WINS|DHCP|GATEWAY 次に例を示します。 `cscript ICMNetworkIsolation.vbe /removeBoundary GATEWAY`	指定されたデバイスを境界デバイスリストから削除します。 このタイプは、DNS、WINS、DHCP、またはGATEWAYとして指定できます。 このユーティリティは、DNS、WINS、DHCP、および GATEWAY をそれぞれドメインネームシステム（DNS）デバイス、Windows インターネット ネーム サービス（WINS）デバイス、Dynamic Host Configuration Protocol（DHCP）デバイス、デフォルトゲートウェイ（GATEWAY）デバイスとして認識します。 Windows は、上記のタイプの各デバイスの IP アドレスの変更を動的に検出し、それに応じて境界フィルタリストを動的に更新します。
	cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary <Outbound|Inbound> <TCP|UDP> <PortNumber> 次に例を示します。 `cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary Inbound TCP 5900`	指定された IP アドレスにあるホストデバイスが、次の基準に一致すると、境界デバイスリストから削除されます。 • 指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。 • 指定されたプロトコル（TCP または UDP）の 1 つ。 • インターネットトラフィック用に指定されたポート番号。
	cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary <IP address> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] 次に例を示します。 `cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary 10.86.121.160 Outbound Any`	

引数名	構文と例	機能
		指定されたIPアドレスにあるデバイスで、次の設定がされているものが境界デバイスリストから削除されます。 • （必須）指定された IP アドレス。 （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。 • （必須）指定されたプロトコル（TCP、UDP、ICMP、または任意のプロトコル）の 1 つ。 • （任意）TCP または UDP が指定したプロトコルの場合、任意のポートまたは指定されたポート。
	cscript ICMNetworkIsolation.vbe /removeSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound|Inbound> <TCP|UDP|ICMP|Any> [All|PortNumber] 次に例を示します。 `cscript ICMNetworkIsolation.vbe /removeSubnetBoundary 10.86.0.0.255.255.0.0 Inbound Any`	指定されたIPアドレスにあるすべてのデバイスで、次の設定がされているものが境界デバイスリストから削除されます。 • （必須）次に指定した範囲の開始 IP アドレス。 • （必須）指定されたサブネットマスク。 • （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。 • （必須）指定されたプロトコル（TCP、UDP、ICMP、または任意のプロトコル）の 1 つ。 • （任意）ポートまたは指定されたポート。

引数名	構文と例	機能
DISABLE POLICY	`cscript ICMNetworkIsolation.vbe /disablePolicy`	コンピュータ上の Unified ICM ネットワーク分離 IPSec ポリシーを無効にします。ただし、ポリシーは削除されません。再有効化は可能です。 このオプションは、ネットワークの問題のトラブルシューティングに役立ちます。 ネットワーク接続に問題がある場合で、原因が分からない場合は、問題の原因を明確にするためにポリシーを無効にしてください。ポリシーが無効な状態でも問題が解決しない場合は、ポリシーが問題の原因ではありません。
DELETE POLICY	`cscript ICMNetworkIsolation.vbe /deletePolicy`	Windows IPSec ポリシーストアから Unified ICM ネットワーク分離セキュリティポリシーを削除し、XML ファイルの名前を CiscoICMIPsecConfig.xml.lastconfig に変更します。

ネットワーク分離 IPSec ポリシーのトラブルシューティング

ネットワーク分離 IPSec ポリシーのトラブルシューティングを行う場合は、次の手順を使用します。

手順

ステップ 1 ポリシーを無効にして、発生したネットワークの問題がまだ存在するかどうかを確認します。ポリシーをシャットダウンすると、高度に分散されたシステムではオプションとして使用できない場合があります。そのため、Unified ICM アプリケーションの設定とテストの後にポリシーを導入することが重要です。

ステップ 2 ポリシーの導入後に、境界デバイスの一覧で指定されている IP アドレスまたはポートが変更されたかどうかを確認します。

ステップ 3 通信パスが信頼済みおよび境界に設定されているかどうかを確認します。両方が重複すると、通信が失敗します。

ステップ 4 <システムドライブ>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML ファイルを参照して、必要な境界デバイスが境界デバイスとしてリストされているかどうかを確認します。セキュリティウィザードを使用して、境界デバイスを確認します。

ステップ 5 Windows MMC コンソールから直接 IPSec ポリシーに加えた変更は、ユーティリティ（またはセキュリティウィザード）には反映されません。[ポリシーの有効化（Enable Policy）] オプションは、常に、XML ファイルに保存されている設定で IPSec ポリシーの保存内容を上書きします。

ステップ 6 記載されている警告を確認してください。