IPSec および NAT のサポート

IPSec の概要

Internet Protocol Security（IPSec）は、暗号セキュリティサービスを使用して、Internet Protocol（IP）ネットワーク上のプライベートで安全な通信を確保するためのオープンスタンダードのフレームワークです。

（注） IPSec はさまざまな方法で導入できます。この章では、IPSec が何であり、IPSec を使用して選択した通信パスを保護する方法について説明します。「ネットワーク分離ユーティリティを使用した IPSec」の章では、サーバとの間のトラフィック**全体**を保護するための、より制限された、けれど自動化された IPSec のアプリケーションについて説明します。ネットワーク分離ユーティリティでは、IPSec の適用作業も保存されます。このユーティリティを使用して IPSec を適用する場合でも、この章を読んで IPSec 導入オプションを理解してください。その後、お使いの環境に対して最もメリットの高いツールを使用できます。

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。

コンタクトセンター環境に IPSec を実装すると、導入の容易さ、使いやすさ、および不正なアクセスから機密情報を保護するバランスを見つけ出すことを意味します。

適切なバランスを見つけ出すには、次の条件が必要です。

- リスクを評価し、組織に適したレベルのセキュリティを判断します。
- 機密情報を識別します。
- リスク管理基準を使用し、特定の情報を保護するセキュリティポリシーを定義します。
- 既存の組織内でポリシーを最適に実装する方法を決定します。
- 管理と技術の要件を確実に満たすようにします。

アプリケーションの使用または導入方法は、セキュリティに関する検討事項に影響します。たとえば、必要なセキュリティは、単一のメインサイトの導入と、信頼されたネットワークをまたがって通信できない複数のサイトにわたる導入の間で異なります。Windows Server のセキュリティ フレームワークは、厳格なセキュリティ要件を満たすように設計されています。ただし、慎重な計画とアセスメント、効果的なセキュリティガイドライン、実施、監査、および適切なセキュリティポリシーの設計と割り当てなしには、ソフトウェア単独では効果的ではありません。

IPSec を有効にした場合、パフォーマンスに影響を及ぼす影響は無視できると予想されます。コール処理レートに影響はありません。：

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

トンネルモードでの IPSec のサポート

データおよび音声ネットワークの導入におけるセキュリティ上の懸念が高いため、Unified ICM と Unified CCE は、セントラル コントローラ サイトとリモート周辺機器（PG）サイト間で IPSec をサポートしています。この安全なネットワーク実装は、WAN 接続が IPSec のトンネルで保護される分散モデルを意味します。トンネルモードの Cisco IOS IPsec の設定とは、2 つのサイト間の Cisco IP ルータ（IPSec ピア）だけが安全なチャネル確立の一部であることを意味します。すべてのデータトラフィックは WAN リンクを通して暗号化されますが、ローカルエリアネットワークでは暗号化されません。トンネルモードは、IPSec ピア間のトラフィックフローの機密性を保証します。これは、IOS ルータが、セントラルサイトをリモートサイトに接続しています。

IPSec 設定の適格な仕様は次のとおりです。

- AES 128
- AES 256

一般に、QoS ネットワークでは、トラフィックがトンネルにカプセル化され、暗号化される前に、パケットヘッダー情報に基づいて QoS 機能を分類および適用します。

転送モードでの IPSec のサポート

システム要件

トランスポートモードでの IPSec のサポートについては、Microsoft Windows Server をインストールする必要があります。

サポートされる通信パス

Unified ICM リリース は、サーバ間の通信を保護するために、Window サーバのオペレーティング環境での IPSec の導入をサポートしています。サポートは、顧客センシティブデータを交換する次のノードリストに制限されています。

1. NAM ルータと CICM ルータ間の接続
2. 冗長な Unified ICM ルータ/ロガーペア間のパブリック接続
3. 冗長な Unified ICM ルータ/ロガーペア間のプライベート接続
4. Unified ICM ルータと Unified ICM 周辺機器ゲートウェイ（PG）間のすべての接続
5. 冗長な Unified ICM ルータ/ロガーのペアと管理者 & データサーバ（プライマリ/セカンダリ）と履歴データサーバ（HDS）間のすべての接続
6. 冗長な Unified ICM ルータ/ロガーペアと管理サーバ、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（プライマリ/セカンダリ）間のすべての接続
7. 冗長な Unified ICM PG ペア間のパブリック接続とプライベート接続
8. Unified CCE 導入における冗長な Unified ICM PG ペアと Unified Communications Manager 間の接続

これらすべてのサーバ通信パスについて、IPSec 導入を計画する際の一般的な基盤として高いセキュリティレベルを検討してください。

IPSec ポリシーの設定

Windows Server IPSec ポリシー設定は、セキュリティ要件を 1 つ以上の IPSec ポリシーに変換することです。

各 IPSec ポリシーは、1 つ以上の IPSec ルールで構成されています。各 IPSec ルールは、次で構成されます。

- 選択したフィルタリスト
- 選択したフィルタアクション
- 選択した認証方式

- 選択した接続タイプ
- 選択したトンネル設定

IPSecポリシーを設定するには複数の方法がありますが、最も直接的な方法は次のとおりです。

新しいポリシーを作成し、必要に応じてフィルタリストとフィルタアクションを追加し、ポリシーのルールを定義します。この方式では、最初にIPSecポリシーを作成してから、ルールを追加および設定します。ルールの作成中に、フィルタリスト（トラフィックタイプの指定）とフィルタアクション（トラフィックの処理方法を指定）を追加します。

各通信パスと各端（各サーバ）に対して、IPSecセキュリティポリシーを作成する必要があります。IP セキュリティ ポリシー ウィザードを使用して各 IPSec ポリシーのプロパティを作成および編集する場合は、次の情報を入力します。

1. 名前
2. [説明（Description）]（任意）
3. デフォルトの応答ルールをアクティブ化しない
4. IP セキュリティルール（追加ウィザードを使用したルールの追加）
   - トンネルのエンドポイント（トンネルを指定しない）
   - ネットワークタイプ：すべてのネットワーク接続
5. IPフィルタリスト
   - 名前
   - [説明（Description）]（任意）
   - 追加ウィザードを使用して IP フィルタを追加します。

     [説明（Description）]（任意）

     送信元アドレス：特定の IP アドレス（パスによって異なります）

     宛先アドレス：特定の IP アドレス（パスによって異なります）

     IP プロトコル の種類：任意
   - 追加ウィザードを使用して IP フィルタアクションを追加します。

     名前

     [説明（Description）]（任意）

     フィルタアクションの一般オプション：セキュリティのネゴシエート

     IPSec をサポートしていないコンピュータと通信しない

     IP トラフィックセキュリティ：整合性と暗号化 - 整合性アルゴリズム：SHA1 - 暗号化アルゴリズム：3DES
   - 認証方法：Active Directory _Kerberos V5 プロトコル（デフォルト）

（注）

- X.509 証明書は、顧客の設定に応じて実稼働環境でも使用できます。Unified ICM がすべての導入モデルで Active Directory を要求する場合、認証方式として Kerberos を使用する場合に、追加のセキュリティ資格情報管理は不要です。PG を介した Unified CM 接続の場合は、事前共有キー（PSK）を使用します。
- セキュリティを強化する際、PSK 認証は相対的に弱い認証方式なので使用しないでください。また、PSK はプレーンテキストで保存されます。テストには PSK のみを使用します。詳細については、事前共有キー認証に関する Microsoft Technet の項目を参照してください。
- IPSec ポリシーをカスタマイズする場合は、IPSec 設定を変更してカスタマイズできます。詳細については、データ保護の設定（クイックモード）設定に関する Microsoft のドキュメントを参照してください。

6. キー交換のセキュリティ方式：IKE セキュリティアルゴリズム（デフォルト）
   - 整合性アルゴリズム：SHA1
   - 暗号化アルゴリズム：3DES
   - Diffie-Hellman グループ：中（DH グループ 2、1024 ビットキー）

（注）

- セキュリティを強化するには、2048 ビット以上の Diffie-Hellman キーを使用して LogJam の脆弱性攻撃による脅威を軽減します（CVE - CVE-2015-4000）。詳細については、https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000を参照してください。強力な Diffie-Hellman グループと長いキー長を組み合わせると、秘密鍵の計算上の困難さが増します。詳細については、キー交換方法に関する Microsoft Technet の項目を参照してください。
- 長いキー長を使用すると、CPU 処理のオーバーヘッドが大きくなります。

Unified Communications Manager への IPSec 接続

Unified Communications Manager が Unified ICM システムと同じドメインにはない Unified CCE システムでは、認証に Kerberos を使用できません。このようなシステムには、X.509 証明書を使用します。

IPSec アクティビティ

IPSec モニタ

Windows Server オペレーティングシステム上の IPSec をモニタするには、IP Security モニタ（ipsecmon）を使用できます。IPSec モニタの詳細については、Microsoft Technet の項目を参照してください。

IPSec ロギングの有効化

ポリシーが正常に動作しない場合は、IPSec セキュリティ関連プロセスのロギングを有効にできます。このログは、Oakley ログと呼ばれます。ログは読みにくいですが、プロセスの失敗の場所を追跡するのに役立ちます。次の手順では、IPSec ロギングを有効にします。

手順

ステップ 1 **[開始（Start）]** > **[実行（Run）]** の順に選択します。

ステップ 2 **Regedt32** と入力 して **[OK]** をクリックして、登録エディタに入ります。

ステップ 3 **HKEY_LOCAL_MACHINE** をダブルクリックします。

ステップ 4 `System\CurrentControlSet\Services\PolicyAgent` に移動します。

ステップ 5 **[ポリシーエージェント（Policy Agent）]** をダブルクリックします。

ステップ 6 右側のペインを右クリックし、**[編集（Edit）]** > **[キーの追加（Add Key）]** を選択します。

ステップ 7 キー名として**Oakley**を入力します（大文字と小文字が区別されます）。

ステップ 8 **[Oakley]** をダブルクリックします。

ステップ 9 左側のペインを右クリックし、**[新規（New）]** > **[DWORD 値（DWORD Value）]** を選択します。

ステップ 10 値の名前 **EnableLogging** を入力します（大文字と小文字が区別されます）。

ステップ 11 値をダブルクリックして、DWORD を **1** に設定します。

ステップ 12 [OK] をクリックします。

ステップ 13 コマンドプロンプトに移動し、**net stop policyagent & net start policyagent** と入力します。

ステップ 14 `%windir%\debug\Oakley.log` でログを検索します。

Message Analyzer

Message Analyzer を使用すると、プロトコル メッセージング トラフィックをキャプチャ、表示、および解析できます。さらに、Windows コンポーネントからのシステムイベントおよび他のメッセージのトレースと評価を行います。

Message Analyzer のダウンロードおよび詳細については、https://www.microsoft.com/en-in/download/details.aspx?id=44226 を参照してください。

システム モニタリング

組み込みのパフォーマンス コンソール（perfmon）を使用すると、ネットワーク アクティビティを他のシステム パフォーマンス データと一緒にモニタできます。ネットワーク コンポーネントは別のハードウェアリソースとして取り扱い、通常のパフォーマンスモニタリングルーチンの一部として確認します。

ネットワーク アクティビティは、ネットワーク コンポーネントだけでなく、システム全体のパフォーマンスにも影響を及ぼす可能性があります。ディスク、メモリ、プロセッサアクティビティなどのネットワーク アクティビティと共に、他のリソースを必ずモニタしてください。システムモニタを使用すると、単一のツールを使用してネットワークとシステムのアクティビティを追跡できます。通常のモニタリング設定の一部として、次のカウンタを使用します。

- Cache\Data Map Hits %
- Cache\Fast Reads/sec
- Cache\Lazy Write Pages/sec
- Logical Disk\% Disk Space
- Memory\Available Bytes
- Memory\Nonpaged Pool Allocs
- Memory\Nonpaged Pool Bytes
- Memory\Paged Pool Allocs
- Memory\Paged Pool Bytes
- Processor(_Total)\% Processor Time
- System\Context Switches/sec
- System\Processor Queue Length
- Processor(_Total)\Interrupts/sec

NAT のサポート

ネットワークアドレス変換（NAT）は、大規模ネットワーク内の登録済み IP アドレスを保存し、IP アドレッシング管理タスクをシンプル化するためのメカニズムです。NAT は、プライベート内部ネットワーク内の IP アドレスを、パブリック外部ネットワーク（インターネットなど）を通じて転送する法律上の IP アドレスに変換します。NAT はさらに、着信トラフィックの法律上 の 配信アドレスを内部ネットワーク内の IP アドレスに変換します。

NAT 全体にわたって Unified CCE 環境に IP 電話を導入できます。リモート周辺機器（PG）サーバは、NAT ネットワークリモートの中央コントローラサーバ（ルータおよびロガー）から見つけ出すことができます。PG サーバの NAT サポート資格は、NAT 機能を備える Cisco IP ルータを実装するネットワーク インフラストラクチャに限定されています。

エージェントデスクトップは、サイレントモニタリングが使用される場合を除き、NAT 環境でサポートされます。サイレントモニタリングは、NAT ではサポートされていません。

NAT の設定方法の詳細については、https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml を参照してください。

NAT 全体に IP 電話を導入する方法の詳細については、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book.pdf を参照してください。

IPSec と NAT の透過性

IPSec NAT の透過表示機能では、NAT と IPSec の間で既知の多くの非互換性に対処することで、ネットワーク内の NAT またはポートアドレス変換（PAT）ポイントを経由する IPSec トラフィックのサポートが導入されます。VPN デバイスは、NAT トラバーサル（NAT-T）を自動的に検出します。両方の VPN デバイスが NAT-T に対応している場合、NAT-T は自動的に検出され、自動的にネゴシエートされます。

その他の IPSec リファレンス

- IPSec アーキテクチャ：https://technet.microsoft.com/en-us/library/bb726946.aspx
- Windows Server：https://docs.microsoft.com/en-us/windows-server/get-started/server-basics
- Windows ファイアウォールおよび IPSec：https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security