Cisco IOS XE強化ガイドの使用

内容

はじめに

このドキュメントでは、Cisco IOS® XEシステムデバイスを保護するための情報について説明します。これにより、ネットワークドキュメントの全体的なセキュリティが向上します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントは、ネットワークデバイスの機能を分類できる3つのプレーンを中心に構成されており、それぞれの機能の概要と関連項目への参照を提供します。

ネットワークの3つの機能プレーン（管理プレーン、コントロールプレーン、およびデータプレーン）は、それぞれ保護が必要な異なる機能を提供します。

1. 管理プレーン：管理プレーンでは、Cisco IOS XEデバイスに送信されるトラフィックが管理されます。管理プレーンを構成するのは、アプリケーション、およびセキュアシェル(SSH)、Simple Network Management Protocol(SNMP)などのプロトコルです。
2. コントロール プレーン：ネットワーク デバイスのコントロール プレーンでは、ネットワーク インフラストラクチャの機能性の維持に重要なトラフィックが処理されます。コントロール プレーンを構成するのは、ネットワーク デバイス間のアプリケーションおよびプロトコルです。Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、Enhanced Interior Gateway Routing Protocol（EIGRP）や Open Shortest Path First（OSPF）などの Interior Gateway Protocol（IGP）が、これに含まれます。
3. データ プレーン：データ プレーンでは、データがネットワーク デバイス経由で転送されます。データプレーンには、ローカルCisco IOS XEデバイスに送信されるトラフィックは含まれません。

このドキュメントで扱うセキュリティ機能に関しては、多くの場合、その機能を設定するために十分な情報を提供しています。しかし、このドキュメントだけでは不十分な場合、それ以上の注意が必要かどうかを判断できるように説明しています。このドキュメントには、実装すればネットワークの保護に役立つ推奨事項が必要に応じて記載されています。

セキュアな運用

セキュアなネットワーク動作は、重要な課題です。このドキュメントの大部分はCisco IOS XEデバイスの安全な設定に関するものですが、ネットワークを完全に保護できるのは設定だけではありません。基本となるデバイスのコンフィギュレーション同様に、ネットワークで使用される操作手順も、セキュリティにとって大きな役割を果たします。

下記のトピックに含まれる操作上の推奨事項を実装することを推奨いたします。下記のトピックでは、ネットワーク動作の重要領域に個別に焦点を当てていますが、すべてを網羅しているわけではありません。

Cisco セキュリティ アドバイザリおよびレスポンスの監視

Cisco Product Security Incident Response Team（PSIRT）は、Cisco 製品のセキュリティ関連問題に関して、PSIRT アドバイザリと呼ばれる通知を作成し、維持しています。あまり重大ではない問題の通知には、Cisco Security Response が使用されます。セキュリティアドバイザリとレスポンスは、『シスコセキュリティアドバイザリとレスポンス』で入手できます。

通知方法についての詳細は、『Ciscoセキュリティ脆弱性ポリシー』を参照してください

セキュアなネットワークを維持するために、リリース済みの Cisco セキュリティ アドバイザリおよびレスポンスに注意する必要があります。ネットワークを危険にさらしかねない脅威を評価できるように、脆弱性に関して知っておく必要があります。この評価プロセスについては、『セキュリティ脆弱性のリスクトリアージに関するアナウンス』を参照してください。

認証、認可、アカウンティングの活用

ネットワーク デバイスをセキュリティで保護するには認証、認可、およびアカウンティング（AAA）フレームワークが重要です。AAA フレームワークでは、管理セッションの認証が行われると同時に、特定の管理者定義コマンドに対してユーザが制限され、すべてのユーザが入力したすべてのコマンドが記録されます。AAA の利用については、このドキュメントの「認証、認可、アカウンティングの使用」の項を参照してください。

ログ収集とモニタリングの一元化

セキュリティインシデントに関連する現在、新しいイベント、過去のイベントに関する知識を得るには、イベントロギングと関連付けの統合戦略が必要です。この戦略では、すべてのネットワーク デバイスからのロギングを活用し、事前パッケージングされカスタマイズ可能な相関機能を使用する必要があります。

ロギングの一元化を実装した後は、ログの分析と事象のトラッキングを行うための構造的なアプローチを開発する必要があります。組織のニーズに応じて、ログ データを入念に見直すというシンプルなものから、高度なルールベースの分析までさまざまな方法をとることができます。

Cisco IOS XEネットワークデバイスにロギングを実装する方法についての詳細は、このドキュメントの「ロギングのベストプラクティス」セクションを参照してください。

セキュアなプロトコルの使用（可能な場合）

ネットワーク管理に関する機密データの伝送には、多くのプロトコルが使用されます。可能な場合は、常にセキュアなプロトコルを使用する必要があります。セキュアなプロトコルを選択するというのは、Telnet の代わりに SSH を使用して、認証データと管理情報の両方を暗号化することが含まれます。さらに、コンフィギュレーション データをコピーする場合は、セキュアなファイル転送プロトコルを使用する必要があります。たとえば、FTP や TFTP の代わりに、Secure Copy Protocol（SCP）を使用します。

Cisco IOS XEデバイスの安全な管理についての詳細は、このドキュメントの「インタラクティブ管理セッションの保護」セクションを参照してください。

NetFlow によるトラフィック情報の取得

NetFlow をイネーブルにすると、ネットワークのトラフィック フローを監視できます。NetFlow の本来の目的は、ネットワーク管理アプリケーションにトラフィック情報をエクスポートすることですが、ルータ上のフロー情報の表示にも使用できます。この機能によって、ネットワークをどのようなトラフィックが通過しているかをリアルタイムで表示できます。フロー情報がリモート コレクタにエクスポートされているかどうかにかかわらず、NetFlow を必要に応じてリアクティブに使用できるようにネットワーク デバイスを設定するように推奨いたします。

この機能についての詳細は、このドキュメントの「トラフィックの識別とトレースバック」セクションおよび「Cisco IOS NetFlow」（登録ユーザ専用）を参照してください。

構成管理

コンフィギュレーション管理は、コンフィギュレーションの変更を提案、検討、承認、および展開するプロセスです。Cisco IOS XEデバイス構成では、構成管理の2つの側面（構成アーカイブとセキュリティ）が重要です。

コンフィギュレーション アーカイブを使用すると、ネットワーク デバイスの変更を元に戻すことができます。セキュリティに関しても、コンフィギュレーション アーカイブを使用して、セキュリティの変更点やその時期を特定できます。この情報を AAA のログ データと組み合わせて使用すると、ネットワーク デバイスのセキュリティ監査に役立ちます。

Cisco IOS XEデバイスの設定には、多くの機密情報が含まれています。たとえば、ユーザ名、パスワード、アクセス コントロール リストの内容が、この種の情報に相当します。Cisco IOS XEデバイス設定をアーカイブするために使用するリポジトリは、セキュリティ保護されている必要があります。この情報へのアクセスがセキュリティで保護されていない場合、ネットワーク全体のセキュリティが損なわれる可能性があります。

管理プレーン

管理プレーンは、ネットワークの管理目標を実現する機能で構成されます。

SSH を使用するインタラクティブ管理セッションや、SNMP または NetFlow による統計情報収

集がこれに含まれます。ネットワーク デバイスのセキュリティを検討する場合、管理プレーンを保護することが不可欠です。セキュリティ上の事象によって管理プレーンの機能が弱体化した場合、ネットワークの回復や安定化ができなくなる可能性があります。

ここでは、管理プレーンの強化に役立つCisco IOS XEソフトウェアで使用可能なセキュリティ機能と設定について詳しく説明します。

管理プレーン全般の強化

管理プレーンは、デバイスのアクセス、コンフィギュレーション、および管理や、デバイス動作の監視とデバイスが展開されているネットワークの監視に使用されます。管理プレーンは、このような機能の動作によるトラフィックを送受信するプレーンです。管理プレーンの動作にはコントロール プレーンの動作が直接影響するので、デバイスの管理プレーンとコントロール プレーンの両方を保護する必要があります。次に、管理プレーンで使用されるプロトコルを示します。

1. Simple Network Management Protocol
2. Telnet
3. Secure Shell Protocol（SSH）
4. File Transfer Protocol（ファイル転送プロトコル）の略。
5. ハイパーテキスト転送プロトコル/セキュアハイパーテキスト転送プロトコル
6. トリビアル ファイル転送プロトコル（TFTP）（Trivial File Transfer Protocol）# とりびあるふぁいるてんそうぷろとこるTFTP #
7. Secure Copy （SCP）プロトコル
8. TACACS+
9. RADIUS
10. NetFlow
11. ネットワーク タイム プロトコル
12. Syslog

    セキュリティ障害の発生時に管理プレーンとコントロール プレーンに影響が及ばないように、手段を講じる必要があります。どちらかのプレーンが悪用されれば、すべてのプレーンのセキュリティが侵害される可能性があります。

パスワード管理

パスワードにより、リソースやデバイスへのアクセスが制御されます。これは、要求の認証に使用されるパスワードまたはシークレットの定義によって実現されます。リソースまたはデバイスへのアクセス要求が受信されると、その要求に対してパスワードと ID の検証が行われ、その結果でアクセスが許可、拒否、または制限されます。セキュリティのベスト プラクティスとして、パスワードの管理には TACACS+ または RADIUS 認証サーバを使用する必要があります。しかし、TACACS+ または RADIUS サービスに障害が発生した場合に備えて、特権アクセス用にローカル設定されたパスワードが依然として必要です。また、デバイスのコンフィギュレーション内には、NTP キー、SNMP コミュニティ ストリング、ルーティング プロトコル キーなど、他のパスワード情報が存在することもあります。

enable secretコマンドを使用すると、Cisco IOS XEシステムへの特権管理アクセスを許可するパ

スワードを設定できます。古い enable password コマンドではなく、enable secret を使用してください。enable password コマンドには、脆弱な暗号化アルゴリズムが使用されています。

enable secret が設定されていない場合にコンソール tty 回線用のパスワードを設定すると、リモートのバーチャル ターミナル（vty）セッションからでも、コンソール パスワードを使用して特権アクセスを取得できます。しかしこれは望ましくないことであり、これも enable secret を設定する理由の一つです。

service password-encryptionグローバルコンフィギュレーションコマンドは、Cisco IOS XEソフトウェアに対して、パスワード、Challenge Handshake Authentication Protocol(CHAP)シークレット、およびコンフィギュレーションファイルに保存されている同様のデータを暗号化するように指示します。このような暗号化を使用すれば、たとえばユーザが何気なく管理者の肩越しに画面を見てパスワードを読み取るといった事態を防止できます。ただし、service password-encryption コマンドで使用されるアルゴリズムは、単純な Vigenere 暗号です。このアルゴリズムは、ある程度高度な知識を持つ攻撃者による本格的な分析からコンフィギュレーション ファイルを保護する設計にはなっていないため、このような目的では使用しないでください。暗号化されたパスワードを含むCisco IOS XEコンフィギュレーションファイルは、同じパスワードのクリアテキストのリストに使用されるのと同じ注意を払って扱う必要があります。

この脆弱な暗号化アルゴリズムは、enable secret コマンドでは使用されていませんが、enable password グローバル コンフィギュレーション コマンドや password ライン コンフィギュレーション コマンドでは使用されています。この種類のパスワードは使用せず、enable secret コマンドか、拡張パスワード セキュリティ機能を使用してください。

enable secret コマンドと拡張パスワード セキュリティ機能では、パスワードのハッシングに Message Digest 5（MD5）が使用されています。このアルゴリズムは十分に公開審査がなされたもので、解読不可能とされています。ただし、このアルゴリズムも辞書攻撃の対象にはなります。辞書攻撃とは、攻撃者が辞書やパスワードの候補を記したリストに掲載されているすべての単語を順に試して一致を調べる手法です。したがって、コンフィギュレーション ファイルは安全な場所に保管し、信頼できる相手とだけ共有するようにしてください。

高度パスワード セキュリティ

拡張パスワードセキュリティ機能はCisco IOS XEソフトウェアリリース16.6.4から導入されており、この機能を使用すると、usernameコマンドでパスワードにMD5ハッシングを適用できます。この機能が登場する以前は、クリアテキストのパスワードであるタイプ0と、Vigenによる暗号化のアルゴリズムを使用するタイプ7の2種類のパスワードがありました。拡張パスワード セキュリティ機能は、取得にクリアテキスト パスワードが必要なプロトコル（CHAP など）では使用しないでください。

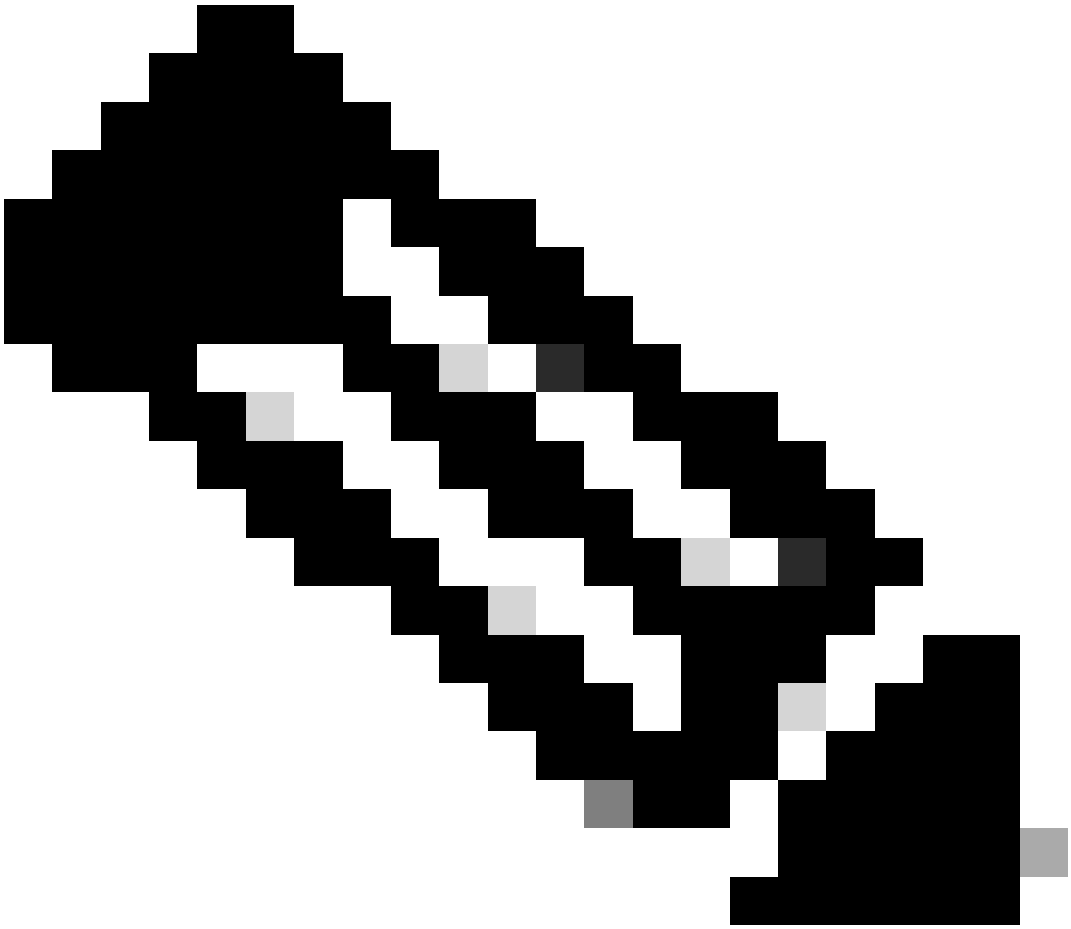
ユーザ パスワードを MD5 ハッシングで暗号化するには、username secret グローバル コンフィギュレーション コマンドを発行します。

username <名前> secret <パスワード>

ログイン パスワードのリトライ ロックアウト

ログインパスワードリトライロックアウト機能はCisco IOS XEソフトウェアリリース16.6.4の最

初のリリースから機能しており、設定した回数だけログインに失敗するとローカルユーザアカウントをロックアウトできます。ロックアウトされたユーザのアカウントは、解除されるまでロックアウト状態になります。特権レベル 15 に設定された認可ユーザを、この機能でロックアウトすることはできません。特権レベル 15 を持つユーザの数は、最小限にとどめる必要があります。



> 注：認証ユーザは、ログイン試行の失敗回数に達すると、デバイスから自分自身をロックアウトできます。また、悪意のあるユーザが、有効なユーザ名を使用して何度も認証を試行することで、サービス拒絶（DoS）状態を作成する可能性があります。

次の例では、ログイン パスワード リトライ ロックアウト機能をイネーブルにする方法を示しています。

aaa new-model aaa local authentication attempts max-fail <max-attempts> aaa authentication login default local

username <名前> secret <パスワード>

この機能は、CHAP やパスワード認証プロトコル（PAP）などの認証方式にも適用できます。

ノー サービス パスワード回復

Cisco IOS XEソフトウェアリリース16.6.4以降では、パスワード回復のディセーブル化機能により、コンソールにアクセスできる任意のユーザが、安全でない方法でデバイス設定にアクセスしてパスワードをクリアすることはできません。また、悪意のあるユーザがコンフィギュレーション レジスタの値を変更したり、NVRAM にアクセスしたりすることもできなくなります。

パスワード回復のディセーブル化

Cisco IOS XEソフトウェアは、ROMモニタモード(ROMMON)へのアクセスに依存し、システムの起動時にブレークキーを使用するパスワード回復手順を提供します。ROMmon モードでは、デバイス ソフトウェアがリロードされ、新しいパスワードを含む新しいシステム コンフィギュレーションにするためのプロンプトを表示できます。

現在のパスワード回復手順では、コンソールにアクセスできる任意のユーザが、デバイスとそのネットワークにアクセスできます。パスワード回復のディセーブル化機能により、システム起動時に Break キー シーケンスが中断され ROMmon に入ることができなくなります。

デバイスに対して no service password-recovery をイネーブルにする場合は、そのデバイス コンフィギュレーションのオフライン コピーを保存すること、およびコンフィギュレーション アーカイブ ソリューションを実装することを推奨いたします。この機能を有効にした後でCisco IOS XEデバイスのパスワードを回復する必要がある場合は、設定全体が削除されます。

使用していないサービスの無効化

セキュリティ上のベスト プラクティスとして、不要なサービスはすべてディセーブルにする必要があります。これらの不要なサービス(特にユーザデータグラムプロトコル(UDP)を使用するサービス)が正規の目的で使用されることはまれですが、通常はパケットフィルタリングで防御されるDoS攻撃やその他の攻撃を開始するために使用される可能性があります。

TCP および UDP のスモール サービスはディセーブルにする必要があります。提供されるサービスには次のものがあります。

1. echo（ポート番号 7）
2. discard（ポート番号 9）
3. daytime（ポート番号 13）
4. chargen（ポート番号 19）

スモール サービスが悪用されるケースの大部分は、アンチスプーフィング アクセス リストによって回避できるか、または危険性を緩和できますが、ネットワークでアクセス可能な任意のデバイスでは、スモール サービスをディセーブルにする必要があります。スモールサービスは、Cisco IOS XEソフトウェアリリース16.6.4以降ではデフォルトで無効になっています。それより前のソフトウェアでは、no service tcp-small-servers と no service udp-small-servers のグローバル コンフィギュレーション コマンドを発行してディセーブルにできます。

次のサービスは、使用しない場合はディセーブルにしてください。

5. Finger サービス：ディセーブルにするには、no ip finger グローバル コンフィギュレーション コマンドを発行します。Cisco IOS XEソフトウェアリリース16.1以降では、このサービスはデフォルトで無効になっています。
6. ブートストラップ プロトコル（BOOTP）：ディセーブルにするには、no ip bootp server グローバル コンフィギュレーション コマンドを発行します。Cisco IOS XEソフトウェアリリース16.1以降では、このサービスはデフォルトで無効になっています。
7. Cisco IOS XEソフトウェアリリース16.6.4以降でBOOTPをディセーブルにするには、グローバルコンフィギュレーションモードでip dhcp bootp ignoreコマンドを発行します。これを実行しても、Dynamic Host Configuration Protocol（DHCP）サービスは引き続きイネーブルのままです。
8. DHCP サービス（DHCP リレー サービスが不要な場合）：ディセーブルにするには、グローバル コンフィギュレーション モードで no service dhcp コマンドを発行します。
9. Maintenance Operation Protocol（MOP）サービス：ディセーブルにするには、インターフェイス コンフィギュレーション モードで no mop enabled コマンドを発行します。
10. ドメイン ネーム システム（DNS）サービス：ディセーブルにするには、no ip domain-lookup グローバル コンフィギュレーション コマンドを発行します。
11. パケット アセンブラ/ディスアセンブラ（PA）サービス（X.25 ネットワークで使用）：ディセーブルにするには、グローバル コンフィギュレーション モードで no service pad コマンドを発行します。
12. HTTP サーバおよびセキュア HTTP（HTTPS）サーバ：HTTP サーバをディセーブルにするには、グローバル コンフィギュレーション モードで no ip http server コマンドを発行します。HTTPS サーバをディセーブルにするには、no ip http secure-server グローバル コンフィギュレーション コマンドを発行します。
13. Cisco IOS XEデバイスが起動時にネットワークからコンフィギュレーションを取得する場合を除き、no service configグローバルコンフィギュレーションコマンドを使用する必要があります。これにより、Cisco IOS XEデバイスはTFTPを使用してネットワーク上のコンフィギュレーションファイルを見つけようとしなくなります。
14. Cisco Discovery Protocol（CDP）は、他の CDP 対応デバイスのネイバールータとの隣接関係やネットワーク トポロジを検出するためのネットワーク プロトコルです。CDP は、ネットワーク管理システム（NMS）やトラブルシューティングに使用できます。非信頼ネットワークに接続しているすべてのインターフェイスで、CDP をディセーブルにする必要があります。これは、no cdp enable インターフェイス コマンドで実行できます。また、no cdp run グローバル コンフィギュレーション コマンドを使用する方法でも CDP をディセーブルにできます。悪意のあるユーザが偵察やネットワーク マッピングを行うために、CDP が使用される可能性があることに注意してください。
15. Link Layer Discovery Protocol（LLDP）は、802.1AB で定義された IEEE プロトコルです。LLDP は CDP と似ています。ただし、LLDP では、CDP に対応していないデバイス間の相互運用が可能になります。LLDP は CDP と同じ方法で扱う必要があります。非信頼ネットワークに接続しているすべてのインターフェイスでは、LLDP をディセーブルにしてください。これを行うには、no lldp transmit および no lldp receive インターフェイス コンフィギュレーション コマンドを発行します。LLDP をグローバルでディセーブルにするには、no lldp run グローバル コンフィギュレーション コマンドを発行します。悪意のあるユーザが偵察やネットワーク マッピングを行うために、LLDP が使用される可能性があります。
16. sdflashからのブートをサポートするスイッチでは、フラッシュからのブートによってセキュリティを強化し、no sdflash設定コマンドでsdflashを無効にできます。

EXEC タイムアウト

EXEC コマンド インタープリタがセッションを終了せずにユーザ入力を待機する時間を設定するには、exec-timeout ライン コンフィギュレーション コマンドを発行します。アイドル状態の vty 回線または tty 回線のセッションをログアウトさせるには、exec-timeout コマンドを使用します。デフォルトでは、非アクティブな状態が10分間続くと、セッションは接続解除されます。

line con 0

exec-timeout <分> [秒]

line vty 0 4

exec-timeout <分> [秒]

TCP セッションのキープアライブ

service tcp-keepalive-in と service tcp-keepalive-out グローバル コンフィギュレーション コマンドを使用すると、デバイスから TCP セッションのための TCP キープアライブを送信できます。デバイスへの着信接続やデバイスからの発信接続で TCP キープアライブをイネーブルにするには、この設定を使用する必要があります。これにより、接続のリモートエンドにあるデバイスが引き続きアクセス可能であり、ハーフオープンまたは孤立した接続がローカルCisco IOS XEデバイスから削除されます。

servicetcp-keepalives-in

サービスTCPキープアライブ発信

管理インターフェイスの使用

デバイスの管理プレーンは、物理的または論理的管理インターフェイス上のインバンドまたはアウトオブバンドでアクセスできます。ネットワークの停止中にも管理プレーンにアクセスできるように、インバンドとアウトオブバンド両方の管理アクセスが、ネットワーク デバイスごとに存在するのが理想的です。

デバイスへのインバンド アクセスに使用される最も一般的なインターフェイスの一つが、論理ループバック インターフェイスです。ループバック インターフェイスは常にアップ状態ですが、物理インターフェイスの状態は変化することがあり、インターフェイスにアクセスできない可能性があります。ループバック インターフェイスを管理インターフェイスとして各デバイスに追加して、管理プレーン専用にしておくことを推奨いたします。これにより、管理者は管理プレーンでネットワーク全体にポリシーを適用できます。デバイスに設定したループバック インターフェイスは、SSH、SNMP、syslog などの管理プレーン プロトコルによってトラフィックの送受信に使用されます。

interface Loopback0

ip address 192.168.1.1 255.255.255.0

メモリしきい値通知

Cisco IOS XEソフトウェアリリース16.6.4で追加されたメモリしきい値通知機能を使用すると、デバイスのメモリ不足状態を緩和できます。この機能では、これを実現するために、メモリしきい値通知とメモリ予約の2つの方法が使用されます。

デバイス上の空きメモリ量が、設定されたしきい値を下回ったことを通知する場合、メモリしきい値通知によって、ログ メッセージが生成されます。次の設定例では、memory free low-watermark グローバル コンフィギュレーション コマンドでこの機能をイネーブルにする方法を示しています。これにより、空きメモリ量がしきい値を下回ればデバイスで通知が生成され、しきい値を 5 % 上回ると再度通知が生成されます。

メモリ空き口ーウォーターマークプロセッサ<しきい値>

メモリフリー低水準点io <しきい値>

メモリ予約を使用すると、重要な通知のために十分なメモリが確保されます。次の設定例は、この機能をイネーブルにする方法を示しています。これにより、デバイスのメモリが使い果たされていても、管理プロセスが機能し続けることができます。

memory reserve critical <値>

CPU しきい値の通知

Cisco IOS XEソフトウェアリリース16.6.4で導入されたCPUしきい値通知機能を使用すると、デバイスのCPU負荷が設定済みのしきい値を超えたときに、その検出と通知を行うことができます。しきい値を超過した場合、デバイスでは SNMP トラップ メッセージが生成されて、送信されます。Cisco IOS XEソフトウェアでは、上昇しきい値と下降しきい値という2つのCPU使用率しきい値方式がサポートされています。

次の設定例は、上昇しきい値および下降しきい値をイネーブルにして CPU しきい値通知メッセージを生成する方法を示しています。

snmp-server enable traps cpuしきい値

snmp-server host <ホストアドレス> <コミュニティストリング> cpu

process cpu threshold type <type> rising <percentage> interval <seconds> [falling <percentage> interval <seconds>]

process cpu statistics limit entry-percentage <number> [size <seconds>]

ネットワーク タイム プロトコル

Network Time Protocol（NTP; ネットワーク タイム プロトコル）は特に危険というわけではありませんが、不要なサービスはどれでも、攻撃を媒介する可能性があります。NTP が使用されている場合は、信頼できるタイミング ソースを明示的に設定して、適切な認証を使用することが重要です。攻撃の可能性に対するフォレンジック調査や、フェーズ1認証で証明書に依存するVPN接

続の成功など、syslogの目的には、正確で信頼できる時間が必要です。

1. NTP のタイム ゾーン：NTP を設定する場合、タイムスタンプが正確に関連付けられるように、タイム ゾーンを設定する必要があります。国際的に展開されるネットワーク内のデバイスに対してタイム ゾーンを設定するには、通常、2 つの方法があります。一つは、すべてのネットワーク デバイスを Coordinated Universal Time（UTC; 世界標準時）（以前の Greenwich Mean Time（GMT; グリニッジ標準時））に設定する方法です。もう一つは、ネットワーク デバイスをローカルのタイム ゾーンに設定する方法です。この機能の詳細については、シスコの製品ドキュメントの「clock timezone」を参照してください。
2. NTP の認証：NTP の認証を設定すると、信頼できる NTP ピア間で確実に NTP メッセージを交換できます。

   NTP認証を使用する設定例：

   クライアント:

   (config)#ntp authenticate

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

   (config)#ntp server 172.16.1.5 key 5 Server:

   (config)#ntp authenticate

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

インフラストラクチャ ACL によるネットワーク アクセス制限

ネットワーク デバイスとの不正な直接通信の防止を目的として考案されたインフラストラクチャ アクセス コントロール リスト（iACL）は、ネットワークに実装できる最も重要なセキュリティ制御機能の一つです。インフラストラクチャ ACL では、ほぼすべてのネットワーク トラフィックはネットワークそのものを宛先とはしないで、単にネットワークを通過するだけであるという考えを有効に活用しています。

iACL を設定して適用するには、ホストまたはネットワークからネットワーク デバイスへのどの接続を許可する必要があるかを指定します。このような接続の一般的な例として、eBGP、SSH、SNMP などがあります。必要な接続が許可された後、そのインフラストラクチャへの他のすべてのトラフィックは明示的に拒否されます。ネットワークを横断するが、そのインフラストラクチャ デバイスを宛先としていないすべての通過トラフィックは、明示的に許可されます。

iACL による保護は、管理プレーンとコントロール プレーンの両方に関係しています。iACL の実装は、ネットワーク インフラストラクチャ デバイス固有のアドレス指定を使用することで容易に

なります。IP アドレッシングによるセキュリティへの影響についての詳細は、『IP アドレッシングに対するセキュリティ志向アプローチ』を参照してください。

次の iACL 設定例では、iACL 実装プロセスを開始する際のスタート地点として使用する必要がある構造を示しています。

ipアクセスリスト拡張ACL：インフラストラクチャ受信

– ルーティングプロトコルとネットワーク管理に必要な接続を許可します。

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179

permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>

permit tcp host <trusted-management-stations> any eq 22コマンド

permit udp host <trusted-netmgmt-servers> any eq 161を発行します。

---任意のネットワーク デバイスに対するその他の IP トラフィックをすべて拒否します。

deny ip any <インフラストラクチャアドレスレンジ> <ワイルドカードマスク>

---通過トラフィックを許可します。

permit ip any any（任意のIPを許可）

作成した iACL は、非インフラストラクチャ デバイスと接続するすべてのインターフェイスに適用する必要があります。これには、他の組織、リモート アクセス セグメント、ユーザ セグメント、データセンター内のセグメントなどと接続するインターフェイスが含まれます。

インフラストラクチャ ACL についての詳細は、『コアの保護：インフラストラクチャ保護 ACL』を参照してください。

ICMP パケット フィルタリング

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は、IP コントロール プロトコルとしての設計になっています。このため、ICPM で伝送されるメッセージは一般に、TCP プロトコルや IP プロトコルに対して広範囲に影響を及ぼす可能性があります。ネットワーク トラブルシューティング ツールの ping や traceroute では ICMP を使用しますが、ネットワークが正常に動作している場合、外部 ICMP 接続が必要になることはほとんどありません。

Cisco IOS XEソフトウェアには、名前またはタイプとコードによってICMPメッセージを明確にフィルタリングする機能があります。次の例の ACL は、これまでの例のアクセス コントロール エントリ（ACE）と組み合わせて使用する必要があります。これにより、信頼できる管理ステーションと NMS サーバからの ping が許可され、その他の ICMP パケットはすべてブロックされます。

ipアクセスリスト拡張ACL：インフラストラクチャ受信

---信頼できる管理ステーションとサーバからの ICMP エコー（ping）を許可します。

permit icmp host <trusted-management-stations> any echo

permit icmp host <trusted-netmgmt-servers> any echo

---任意のネットワーク デバイスに対するその他の IP トラフィックをすべて拒否します。

deny ip any <インフラストラクチャアドレスレンジ> <ワイルドカードマスク>

---通過トラフィックを許可します。

permit ip any any（任意のIPを許可）

IP フラグメントのフィルタリング

フラグメント化された IP パケットのフィルタリ プロセスでは、セキュリティ デバイスにとって難しい問題があります。これは、TCP パケットと UDP パケットのフィルタリングに使用されるレイヤ 4 情報が、先頭フラグメントにしか存在しないからです。Cisco IOS XEソフトウェアは、特定の方法を使用して、設定されたアクセスリストと先頭以外のフラグメントを照合します。Cisco IOS XEソフトウェアは、ACLに対してこれらの先頭以外のフラグメントを評価し、レイヤ4フィルタリング情報を無視します。これにより、設定された ACE のレイヤ 3 の部分でのみ、先頭以外のフラグメントを評価することになります。

次の設定例では、192.168.1.1 のポート 22 宛の TCP パケットが転送中にフラグメント化された場合、先頭フラグメントは、パケット内のレイヤ 4 情報に基づいて 2 番目の ACE によって期待どおりに廃棄されます。ただし、残り（先頭以外）のフラグメントは、パケットのレイヤ 3 情報と ACE のみに基づいて最初の ACE によって許可されます。このシナリオを次の設定に示します。

ipアクセスリスト拡張ACL-FRAGMENT-EXAMPLE

permit tcp any host 192.168.1.1 eq 80

deny tcp any host 192.168.1.1 eq 22

フラグメント処理はわかりにくいため、ACL により IP フラグメントが誤って許可されることがあります。また、侵入検知システムによる検出を逃れようとして、フラグメンテーションが使用されることもよくあります。このような理由から、IP フラグメントは攻撃で使用されることが多く、設定された iACL の先頭で明示的にフィルタリングを適用する必要があります。次の ACL の例には、あらゆる IP フラグメントのフィルタリングが含まれます。この例の機能は、これまでの例の機能と組み合わせて使用する必要があります。

ipアクセスリスト拡張ACL：インフラストラクチャ受信

– プロトコル固有のACEを使用するIPフラグメントを拒否して、

---IP フラグメントを拒否します。

deny tcp any any fragments（任意のフラグメントを拒否）

deny udp any any fragments（すべてのフラグメントをUDPに拒否）

deny icmp any any fragments（icmpの任意のフラグメント）

deny ip any any fragments（どのフラグメントでも拒否）

---任意のネットワーク デバイスに対するその他の IP トラフィックをすべて拒否します。

deny ip any <インフラストラクチャアドレスレンジ> <ワイルドカードマスク>

---通過トラフィックを許可します。

permit ip any any（任意のIPを許可）

フラグメント化された IP パケットの ACL による処理の詳細は、『アクセス コントロール リストと IP フラグメント』を参照してください。

IP オプションのフィルタリングの ACL サポート

Cisco IOS XEソフトウェアリリース16.6.4では、ACLを使用して、パケットに含まれるIPオプションに基づいてIPパケットをフィルタリングする機能のサポートが追加されました。IP オプションは例外パケットとして処理されるので、ネットワーク デバイスのセキュリティにとって難しい問題です。これには、ネットワークを通過する通常のパケットには必要のないレベルの CPU 作業が必要です。また、パケット内に IP オプションがあるということは、ネットワーク内のセキュリティ制御を無力化させようとしているか、パケットの転送特性を変えようとしていることを示しています。このような理由から、IP オプションがついたパケットは、ネットワークのエッジでフィルタリングする必要があります。

IP オプションを含む IP パケットに対して完全なフィルタリングを行うには、次の例を前の例の ACE と組み合わせて使用する必要があります。

ipアクセスリスト拡張ACL：インフラストラクチャ受信

— IPオプションを含むIPパケットを拒否

deny ip any anyオプションany-options

---任意のネットワーク デバイスに対するその他の IP トラフィックをすべて拒否します。

deny ip any <インフラストラクチャアドレスレンジ> <ワイルドカードマスク>

---通過トラフィックを許可します。

permit ip any any（任意のIPを許可）

ACL の TTL 値フィルタリング サポート

Cisco IOS XEソフトウェアリリース16.6.4では、ACLのサポートが追加され、存続可能時間(TTL)値に基づいてIPパケットがフィルタリングされるようになりました。IP データグラムの TTL 値は、パケットが発信元から宛先へと移動する中で、ネットワーク デバイスを通過するごと

に減少します。初期値はオペレーティング システムによって異なりますが、パケットの TTL が 0 に達すると、そのパケットは廃棄されます。TTL を 0 まで減らすことになったデバイスでは、パケットが廃棄され、ICMP Time Exceeded メッセージが生成されてパケットの発信元に送信されます。

このようなメッセージの生成と送信は、例外プロセスです。期限が切れる IP パケットの数が少ない場合は、ルータでこの機能を実行できますが、期限が切れる IP パケットの数が多い場合、メッセージを生成して送信するために、空いているすべての CPU リソースが使用されます。これは、DoS 攻撃の兆候を示しています。このため、期限が切れる IP パケットの大量発生を利用する DoS 攻撃に対抗するため、デバイスのセキュリティを強化する必要があります。

TTL 値が低い IP パケットは、ネットワークのエッジでフィルタリングすることを推奨いたします。ネットワークの通過するために十分な TTL 値がないパケットを完全にフィルタリングすることで、TTL ベースの攻撃の脅威を緩和できます。

この例では、ACLは6未満のTTL値を持つパケットをフィルタリングします。これにより、5 ホップまでのネットワークは TTL 期限切れ攻撃から保護されます。

ipアクセスリスト拡張ACL：インフラストラクチャ受信

---ネットワークを通過するには不十分な TTL 値が設定された IP パケットを拒否します。

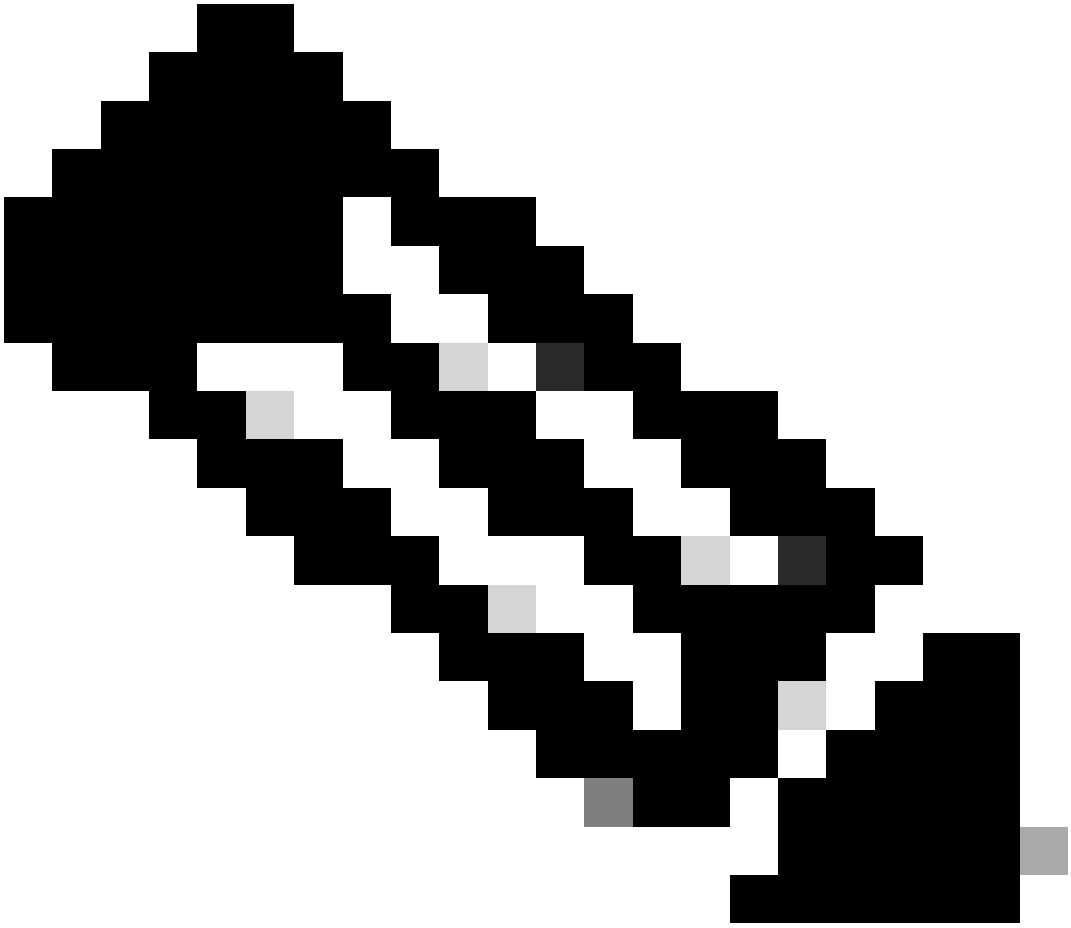
deny ip any any ttl lt 6

---任意のネットワーク デバイスに対するその他の IP トラフィックをすべて拒否します。

deny ip any <インフラストラクチャアドレスレンジ> <マスク>

---通過トラフィックを許可します。

permit ip any any（任意のIPを許可）



注：プロトコルによっては、TTL値が低いパケットを正当な目的で使用するものもあります。eBGPもそのようなプロトコルの1つです。TTL 期限切れに基づいた攻撃を緩和する方法の詳細は、『TTL 超過攻撃の識別と緩和』を参照してください。

インタラクティブ管理セッションの保護

デバイスとの管理セッションでは、デバイスとその動作に関する情報の表示と収集ができます。この情報が悪意のあるユーザに公開されると、そのデバイスが攻撃対象となり、侵入されて、さらなる攻撃に利用される可能性があります。デバイスへの特権アクセスを持つユーザは、そのデバイスに対して全面的な管理制御を行うことができます。情報の漏えいと不正アクセスを防止することはセキュア管理セッションに不可欠です。

管理プレーン保護

Cisco IOS XEソフトウェアリリース16.6.4以降では、管理プレーン保護(MPP)機能を使用して、デバイスが管理トラフィックを受信できるインターフェイスを制限できます。この機能により管

理者は、デバイスとそのアクセス方法に対する制御を強化できます。

次の例は、MPP をイネーブルにして、GigabitEthernet0/1 インターフェイスで SSH と HTTPS のみを許可する方法を示しています。

コントロールプレーンホスト

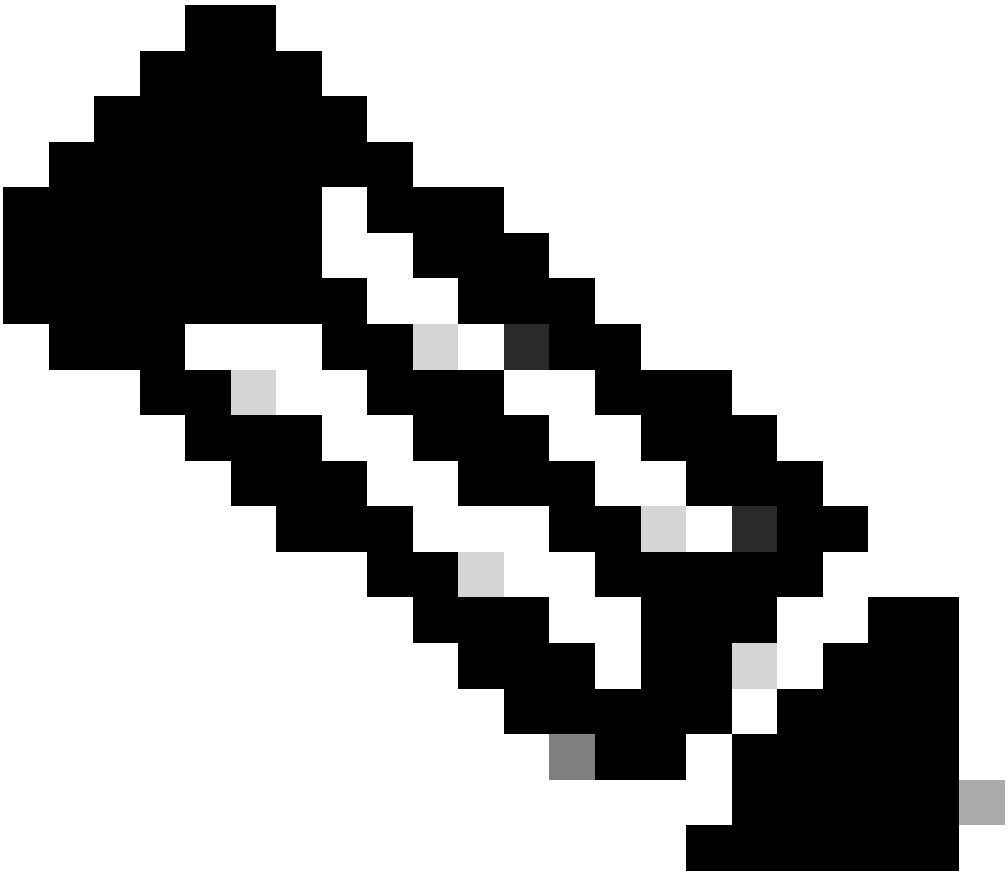
management-interface GigabitEthernet 0/1 allow ssh https（オプション）

コントロール プレーン保護

Control Plane Protection(CPPr)は、コントロールプレーンポリシングの機能を基盤として構築されており、IOS-XEデバイスのルートプロセッサ宛てのコントロールプレーントラフィックを制限およびポリシングします。CPPrは、コントロールプレーンをサブインターフェイスと呼ばれる個別のコントロールプレーンカテゴリに分割します。コントロール プレーンのサブインターフェイスは、Host、Transit、および CEF-Exception の 3 つです。さらに、CPPr には次のコントロールプレーン保護機能が追加されています。

1. ポートフィルタリング機能：閉じているか受信状態ではない TCP ポートや UDP ポートに向かうパケットの規制や廃棄を行います。
2. キューしきい値ポリシー機能：コントロール プレーンの IP 入力キューで許可されている指定されたプロトコルのパケット数を制限します。

   CPPr により管理者は、ホスト サブインターフェイスを使用して管理目的でデバイスに送信されるトラフィックを分類、規制、および制限できます。ホスト サブインターフェイス カテゴリに分類されるパケットの例として、SSH または Telnet などの管理トラフィックや、ルーティング プロトコルがあります。



注:CPPrはIPv6をサポートしておらず、IPv4入力パスに制限されています。

Cisco CPPr機能についての詳細は、『コントロールプレーンポリシング』を参照してください。

管理セッションの暗号化

インタラクティブ管理セッションの実行中は情報が開示される可能性があるので、このトラフィックを暗号化して、悪意のあるユーザが送信中のデータにアクセスできないようにする必要があります。トラフィックを暗号化することで、デバイスとのリモート アクセス接続が保護されます。管理セッションのトラフィックがネットワーク上にクリアテキストで送信された場合、デバイスとネットワークに関する機密情報が攻撃者に取得される可能性があります。

管理者は、SSHまたはセキュアハイパーテキスト転送プロトコル(HTTPS)機能を使用して、デバイスへの暗号化された安全なリモートアクセス管理接続を確立できます。Cisco IOS XEソフトウェアは、SSHバージョン2.0(SSHv2)、およびSecure Sockets Layer(SSL)とTransport Layer Security(TLS)を使用して認証とデータ暗号化を行うHTTPSをサポートしています。

Cisco IOS XEソフトウェアは、Secure Copy Protocol(SCP)もサポートしています。SCPにより、デバイス設定やソフトウェアイメージをコピーするための暗号化された安全な接続が可能にな

ります。SCP では SSH が使用されています。

次の設定例では、Cisco IOS XEデバイスでSSHを有効にしています。

ipドメイン名example.com

暗号キーはrsaモジュラス2048を生成します

ip ssh time-out 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

line vty 0 4

トランスポート入力SSH

次の設定例では、SCP サービスをイネーブルにしています。

ip scp server enable（IPSCPサーバの有効化）

次は、HTTPS サービスの設定例です。

暗号キーはrsaモジュラス2048を生成します

ip http secure-server（セキュアサーバ）

SSHv2

SSHv2機能は、ユーザがSSHv2を設定できる最初のリリース16.6.4でCisco IOS XEに導入されました。SSHは信頼性の高いトランスポート層の上で動作し、強力な認証および暗号化機能を提供します。SSH では、信頼できる転送として定義されているのは TCP のみです。SSH で、ネットワーク上の他のコンピュータ またはデバイスに安全にアクセスしたり、コマンドを安全に実行できます。SSH 経由でトンネリングされる Secure Copy Protocol（SCP）機能により、ファイルを安全に転送できます。

ip ssh verson 2コマンドが明示的に設定されていない場合、Cisco IOS XEはSSHバージョン1.99を有効にします。SSHバージョン1.99では、SSHv1接続とSSHv2接続の両方が許可されます。SSHv1は安全でないと見なされており、システムに悪影響を及ぼす可能性があります。SSHが有効な場合は、ip ssh version 2コマンドを使用してSSHv1を無効にすることをお勧めします。

次の設定例では、Cisco IOS XEデバイスでSSHv2（SSHv1は無効）を有効にしています。

hostname router

ipドメイン名example.com

暗号キーはrsaモジュラス2048を生成します

ip ssh time-out 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

ip sshバージョン2

line vty 0 4

トランスポート入力SSH

SSHv2の使用の詳細については、セキュア シェル バージョン2サポートを参照してください。

RSA キーの SSHv2 拡張機能

Cisco IOS XE SSHv2は、キーボードインタラクティブおよびパスワードベースの認証方式をサポートしています。RSA キーの SSHv2 拡張機能は、クライアントとサーバ向けの RSA ベースの公開キー認証もサポートしています。

ユーザ認証の場合、RSA ベースのユーザ認証では、各ユーザに関連付けられている秘密キー/公開キーのペアを認証に使用します。ユーザは秘密キーと公開キーのペアをクライアントで生成し、Cisco IOS XE SSHサーバで公開キーを設定して、認証を完了する必要があります。

クレデンシャルの確立を試行する SSH ユーザは、秘密キーを使用して暗号化されたシグニチャを提示します。シグニチャとユーザの公開キーは、認証のために SSH サーバに送信されます。SSH サーバでは、ユーザから提示された公開キーに対してハッシュを計算します。ハッシュがサーバと一致するエントリがあるかどうかを判断するために使用されます。一致が見つかった場合、RSA ベースのメッセージ検証が公開キーを使用して実行されます。その結果、暗号化されたシグニチャに基づいて、ユーザのアクセスは認証されるか拒否されます。

サーバ認証では、Cisco IOS XE SSHクライアントが各サーバにホストキーを割り当てる必要があります。クライアントがサーバとの間で SSH セッションを確立しようとすると、キー交換メッセージの一部として、サーバのシグニチャを受信します。厳密なホスト キーのチェック フラグがクライアント側でイネーブルの場合、そのサーバに対応するホスト キー エントリが事前に設定されているかどうかがクライアントで確認されます。一致が見つかると、クライアントはサーバ ホスト キーを使用してシグニチャの検証を試行します。サーバが正常に認証されると、セッションの確立が続行されます。正常に認証されないと、セッションは終了し、「Server Authentication Failed」というメッセージが表示されます。

次の設定例では、Cisco IOS XEデバイスでSSHv2を使用したRSAキーの使用を有効にします。

デバイスのホスト名を設定します

hostname router

ドメイン名の設定

ipドメイン名example.com

を使用するルータで、ローカルおよびリモート認証用にSSHサーバを有効にします。

crypto key generateコマンドを使用します。

SSHバージョン2の場合、モジュラスサイズは768ビット以上である必要があります

crypto key generate rsa usage-keys label sshkeys modulus 2048（暗号キー生成rsaユーセジキーラベルsshkeysモジュラス2048）

SSHに使用するRSAキーペア（この場合は「sshkeys」）の名前を指定します

ip ssh rsaキーペア名sshkeys

sshタイムアウトを設定します（秒単位）。

次の出力では、SSH接続に対して120秒のタイムアウトが有効になっています。

ip ssh time-out 120

認証の再試行回数を5回に制限するように設定します。

ip ssh authentication-retries 5

SSHバージョン2を設定します。

ip sshバージョン2

SSHv2でのRSAキーの使用法の詳細については、『セキュアシェルバージョン2のRSAキーに関する機能拡張』を参照してください。

この設定例では、Cisco IOS XE SSHサーバでRSAベースのユーザ認証を実行できるようにします。サーバに保存されている RSA 公開キーが、クライアントに保存されている公開キーと秘密キーのペアを使用して検証されると、ユーザ認証は成功です。

デバイスのホスト名を設定します。

hostname router

ドメイン名を設定します。

ipドメイン名cisco.com

2048ビットのモジュラスを使用するRSAキーペアを生成します。

暗号キーはrsaモジュラス2048を生成します

SSHサーバでユーザおよびサーバ認証用のSSH-RSAキーを設定します。

ip ssh公開キーチェーン

SSH ユーザ名を設定します。

SSHサーバでユーザおよびサーバ認証用のSSH-RSAキーを設定します。

ip ssh公開キーチェーン

SSH ユーザ名を設定します。

ユーザ名ssh-user

リモート ピアの RSA 公開キーを指定します。

次に、key-stringコマンドのいずれかを設定します

（その後にリモートピアのRSA公開キーが続く）または

key-hashコマンド（続いてSSHキータイプとバージョン）。

SSHv2でのRSAキーの使用法の詳細については、『RSAベースのユーザ認証を実行するためのCisco IOS XE SSHサーバの設定』を参照してください。

この設定例では、Cisco IOS XE SSHクライアントでRSAベースのサーバ認証を実行できるようにします。

hostname router

ip domain-name cisco.com

RSA キー ペアを生成します。

暗号キー生成RSA

SSHサーバでユーザおよびサーバ認証用のSSH-RSAキーを設定します。

ip ssh公開キーチェーン

ルータで公開キー認証のためにSSHサーバを有効にします。

サーバのSSHサーバ名

リモートピアのRSA公開キーを指定します。

次に、key-stringコマンドのいずれかを設定します

（その後にリモートピアのRSA公開キーが続く）または

key-hash <key-type> <key-name>コマンド(その後にSSHキー

タイプとバージョン)。

サーバ認証が実行されていることを確認します。接続は

が障害発生時に終了しました。

ip ssh厳密キーチェック

SSHv2でのRSAキーの使用法の詳細については、『RSAベースのサーバ認証を実行するためのCisco IOS XE SSHクライアントの設定』を参照してください。

コンソール ポートと AUX ポート

Cisco IOS XEデバイスでは、コンソールポートと補助(AUX)ポートは、デバイスへのローカルおよびリモートアクセスに使用できる非同期回線です。Ciscoデバイスのコンソールポートには特別な権限があることに注意してください。特に、管理者はこのような特権を使用して、パスワード回復手順を実行できることには注意が必要です。コンソール ポートにアクセスでき、デバイスへの電力供給を遮断するかデバイスをクラッシュさせることができれば、認証されていない攻撃者でもパスワードの回復を実行できます。

そのため、デバイスのコンソール ポートにアクセスするために使用されるあらゆる方法を、デバイスへの特権アクセスに対するセキュリティと同等に保護する必要があります。アクセス保護に使用される方法としては、AAA、exec-timeout、およびコンソールにモデムが接続されている場合はモデム パスワードがあります。

パスワード回復が不要な場合は、no service password-recoveryグローバルコンフィギュレーションコマンドを使用してパスワード回復手順を実行する機能を削除できます。ただし、no service password-recoveryコマンドがイネーブルにされると、そのデバイスに対するパスワード回復は実行できなくなります。

多くの場合、デバイスの AUX ポートは、不正アクセスを防止するためにディセーブルにする必要があります。AUX ポートをディセーブルにするには、次のコマンドを使用します。

line aux 0

transport input none

transport output none

no exec exec-timeout 0 1

パスワードなし

vty 回線と tty 回線の制御

Cisco IOS XEソフトウェアのインタラクティブ管理セッションは、ttyまたはvirtual tty(vty)を使用します。tty は、デバイスとのローカル アクセス用の端末や、デバイスとのダイヤルアップ アクセス用のモデムと接続できるローカルの非同期回線です。tty はその他のデバイスのコンソール ポートにも接続できます。これにより、tty 回線に接続されたデバイスはコンソール サーバとして機能でき、この状態で、tty 回線に接続されたデバイスのコンソール ポートにネットワークを介して接続を確立できます。ネットワークを経由したこのようなリバース接続の tty 回線も制御する必要があります。

vty 回線は、プロトコルにかかわらず（SSH、SCP、Telnet など）、デバイスによってサポートされるその他のすべてのリモート ネットワーク接続で使用されます。ローカルまたはリモートの

管理セッションを介してデバイスにアクセスできるように、vty 回線および tty 回線の両方を適切に制御する必要があります。Cisco IOS XEデバイスで使用できるvty回線の数は限られています。使用できる回線数は、show line EXECコマンドで確認できます。すべての vty 回線が使用されている場合、新しい管理セッションは確立できません。これにより、デバイスへのアクセスにとっての DoS 状態が発生します。

デバイスの vty または tty に対する最も単純な形式のアクセス コントロールは、ネットワーク内のデバイスの場所にかかわらず、すべての回線で認証を使用することです。vty 回線にはネットワークを介してアクセスできるので、これは vty 回線にとって不可欠です。デバイスへのリモートアクセスに使用されているモデムに接続されている tty 回線や、他のデバイスのコンソール ポートに接続されている tty 回線も、ネットワークを介してアクセスできます。vty および tty のアクセス コントロールを行う他の方法としては、transport input または access-class コンフィギュレーション コマンドを使用する方法、CoPP 機能と CPPr 機能を使用する方法、またはデバイスのインターフェイスにアクセス リストを適用する方法があります。

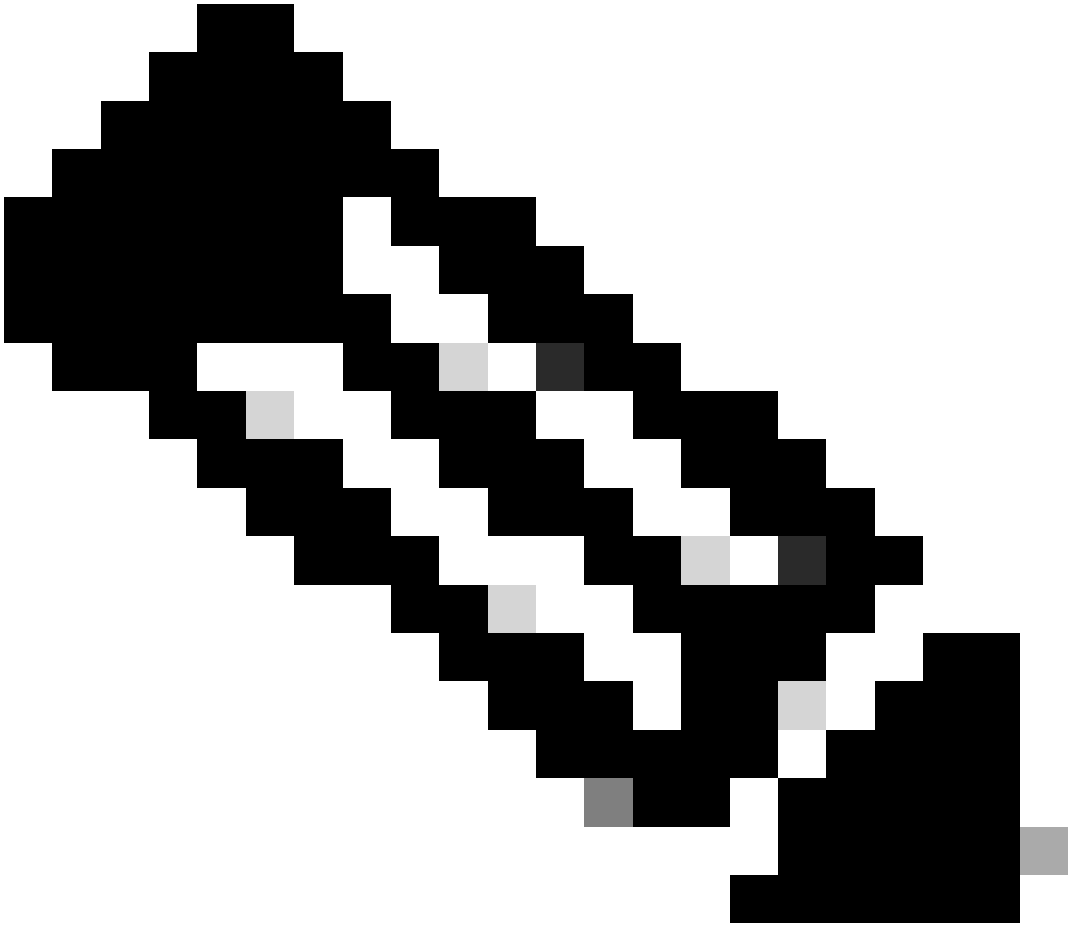
AAA を使用することで認証を実行できます。デバイス アクセスの認証には、ローカル ユーザ データベースを使用するか、または vty 回線や tty 回線に直接設定された単純なパスワード認証を使用して AAA を適用することが推奨されています。

アイドル状態の vty 回線または tty 回線のセッションをログアウトさせるには、exec-timeout コマンドを使用します。また、service tcp-keepalives-in コマンドを使用して、デバイスへの着信接続で TCP キープアライブをイネーブルにすることも必要です。これにより、接続のリモートエンドにあるデバイスが引き続きアクセス可能であり、ハーフオープンまたは孤立した接続がローカルIOS-XEデバイスから削除されます。

vty 回線と tty 回線の転送制御

デバイスがコンソールサーバとして使用されている場合、そのデバイスへの、またはそのデバイスを介した暗号化され安全なリモートアクセス管理接続のみを受け入れるように、vtyとttyを設定できます。このセクションでは tty の場合について説明します。tty 回線は他のデバイス上のコンソール ポートに接続でき、これによりネットワーク経由で tty へのアクセスが可能になるからです。情報の開示や管理者とデバイスの間で送信されるデータへの不正アクセスを防止するために、Telnetやrloginなどのクリアテキストプロトコルを使用する代わりにtransport input sshを使用できます。tty に対しては、transport input none コンフィギュレーションをイネーブルにできます。これにより、事実上リバース コンソール接続で tty 回線を使用できなくなります。

vty 回線と tty 回線はどちらも他のデバイスに接続できます。発信接続に使用できるトランスポートの種類を制限するには、transport output line コンフィギュレーション コマンドを使用します。発信接続が不要の場合は、transport output noneを使用できます。ただし、発信接続を許可する場合は、transport output sshを使用して、暗号化された安全なリモートアクセス方式で接続できます。



注:IPSecは、サポートされている場合、デバイスへの暗号化された安全なリモートアクセス接続に使用できます。IPSec を使用する場合は、デバイスにさらに CPU オーバーヘッドが加わります。ただし、IPSec を使用する場合でも引き続き SSH をトランスポートとして使用する必要があります。

警告バナー

一部の司法管轄地域では、システムの使用が許可されていないことが不正ユーザに通知されていなければ、それらのユーザを訴追することはできず、悪意のあるユーザの監視も不法行為とみなされる場合があります。この通知を行う方法の1つは、Cisco IOS XEソフトウェアのbanner loginコマンドで設定されるバナーメッセージにこの情報を入力することです。

法的通知要件は複雑で、管轄区域や状況によって異なり、弁護士と話し合うことができます。司法管轄地域内でも、複数の法的見解が存在する場合もあります。弁護士とご相談の上、次の情報の一部または全部をバナーに含めることが考えられます。

1. 特別に承認された人のみがシステムへのログインやシステムの使用を許可されていることを

伝える通知と、だれが使用を承認できるのかを示す情報。
2. システムの不正な使用は違法であり、民事罰および刑事罰が課される場合があることを伝える通知。
3. システムのあらゆる使用が、これ以上の警告なしに記録または監視され、その結果得られたログが裁判所での証拠として使用される場合があることを伝える通知。
4. 地域法によって規定されている特定の通知

法的観点よりもセキュリティの観点から、ログインバナーにルータ名、モデル、ソフトウェア、所有権に関する特定の情報を含めることはできません。これらの情報は悪意のあるユーザに利用される可能性があります。

認証、許可、およびアカウンティング

ネットワーク デバイスへのインタラクティブ アクセスをセキュリティ保護するには認証、認可、アカウンティング（AAA）フレームワークが重要です。AAA フレームワークでは、ネットワークのニーズに基づいて詳細に設定できる環境が提供されます。

TACACS+ 認証

TACACS+は、Cisco IOS XEデバイスがリモートAAAサーバに対する管理ユーザの認証に使用できる認証プロトコルです。これらの管理ユーザは、SSH、HTTPS、Telnet、またはHTTPを介してIOS-XEデバイスにアクセスできます。

TACACS+ 認証、またはより一般的に AAA 認証では、各ネットワーク管理者が個々のユーザ アカウントを使用できます。単一の共有パスワードに依存しない場合、ネットワークのセキュリティが向上すると同時に、アカウンタビリティも強化されます。

RADIUSは目的がTACACS+に似たプロトコルです。ただし、ネットワーク経由で送信されるパスワードを暗号化するだけです。一方、TACACS+ では、ユーザ名とパスワードを含む TCP ペイロード全体が暗号化されます。このため、AAAサーバでTACACS+がサポートされている場合、RADIUSよりもTACACS+を使用できます。これら 2 つのプロトコルの詳細な比較は、『TACACS+ と RADIUS の比較』を参照してください。

Cisco IOS XEデバイスでTACACS+認証を有効にするには、次の例のような設定を使用します。

aaa new-model

aaa authentication login default group tacacs+(aaa authentication login default group tacacs+)

tacacsサーバ<server_name>

address ipv4 <tacacs_server_ip_address>（オプション）

キー

この設定は、組織固有の AAA 認証テンプレートの出発点として使用できます。

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャル リストです

。方式リストを使用すると、認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方式が失敗した場合に備えて認証のバックアップ システムを確保できます。Cisco IOS XEソフトウェアは、ユーザを正常に受け入れるか拒否する、リストの最初の方式を使用します。後続の例は、サーバが使用できないか正しくない設定によって以前の方法が試行されます。

名前付き方式リストの設定の詳細については、認証の名前付き方式リストを参照してください。

認証フォールバック

設定されているすべてのTACACS+サーバが使用できなくなった場合、Cisco IOS XEデバイスはセカンダリ認証プロトコルを利用できます。一般的には、設定されたすべての TACACS+ サーバが利用不能になった場合は、ローカル認証かイネーブル認証を使用するように設定します。

オンデバイス認証のオプションは、enable、local、および line です。これらのオプションにはそれぞれの利点があります。enable secret の使用が推奨されます。秘密鍵のハッシュには、回線認証やローカル認証で使用される Type 7 パスワードで使用される暗号化アルゴリズムよりも、本質的にさらに安全な一方向アルゴリズムが使用されるからです。

ただし、ローカルに定義されたユーザのシークレットパスワードの使用をサポートするCisco IOS XEソフトウェアリリースでは、ローカル認証にフォールバックすることが望ましい場合があります。これにより、1 人以上のネットワーク管理者が、ローカル定義ユーザを作成できます。TACACS+ が完全に利用不能になった場合、各管理者はローカルのユーザ名とパスワードを使用できます。この措置によって TACACS+ 停止中のネットワーク管理者のアカウンタビリティが強化されますが、すべてのネットワーク デバイス上のローカル ユーザ アカウントを維持する必要があるので、管理上の負担は飛躍的に大きくなります。

次の設定例では、前の TACACS+ 認証例を踏まえて、enable secret コマンドでローカルに設定されたパスワードへのフォールバック認証が追加されています。

enable secret <password>

aaa new-model

aaa authentication login default group tacacs+ enable（オプション）

tacacsサーバ<server_name>

address ipv4 <tacacs_server_ip_address>（オプション）

キー

AAA でフォールバック認証を使用する方法についての詳細は、『認証の設定』を参照してください。

Type 7 パスワードの使用

Type 7 パスワードは本来、保管されたパスワードを迅速に復号化する設計になっており、パスワードを保管するための安全な形式ではありません。これらのパスワードを簡単に復号化できるツ

ールは多数あります。Type 7パスワードの使用は、Cisco IOS XEデバイスで使用中の機能で必要とされない限り避けることができます。

Type 9(scrypt)は、可能な限り使用できます。

username <username> privilege 15 algorithm-type scrypt secret <secret>

この種類のパスワードをなくすには、AAA 認証や拡張パスワード セキュリティ機能を使用してください。これにより、username グローバル コンフィギュレーション コマンドでローカルに定義されたユーザがシークレット パスワードを使用できます。Type 7 パスワードの使用を完全にはなくせない場合は、これらのパスワードを暗号化するのではなく難読化することを検討してください。

Type 7 パスワードの除去についての詳細は、このドキュメントの「管理プレーン全般の強化」の項を参照してください。

TACACS+ コマンド認可

TACACS+ と AAA によるコマンド認可は、管理ユーザによって入力された各コマンドを許可または拒否するメカニズムです。ユーザがEXECコマンドを入力すると、Cisco IOS XEは各コマンドを設定済みのAAAサーバに送信します。次に、その AAA サーバでは、設定されたポリシーを使用して、その特定のユーザに対してコマンドを許可または拒否します。

前の例の AAA 認証に次の設定を追加すると、コマンド認可を実装できます。

aaa authorization exec default group tacacs+ none

aaa authorization commands 0 default group tacacs+ none

aaa authorizationコマンド1 default group tacacs+ none

aaa authorizationコマンド15 default group tacacs+ none

コマンド認可についての詳細は、『認可の設定』を参照してください。

TACACS+ コマンド アカウンティング

AAA コマンド アカウンティングを設定すると、入力された各 EXEC コマンドに関する情報が、設定された TACACS+ サーバに送信されます。TACACS+ サーバに送信される情報には、実行されたコマンド、実行日、およびコマンドを入力したユーザ名が含まれます。RADIUS ではコマンド アカウンティングはサポートされていません。

次の設定例では、特権レベル 0、1、および 15 で入力された EXEC コマンドに対して AAA コマンド アカウンティングがイネーブルになります。この設定は、TACACS サーバの設定を含む前の例を基にしています。

aaa accounting exec default start-stop group tacacs+（aaaアカウンティングexecデフォルトスタートストップグループtacacs+）

aaa accountingコマンド0 default start-stop group tacacs+

aaa accountingコマンド1 default start-stop group tacacs+

aaa accountingコマンド15 default start-stop group tacacs+

AAA アカウンティングの設定についての詳細は、『アカウンティングの設定』を参照してください。

冗長 AAA サーバ

環境で活用されるAAAサーバは、冗長性を備え、耐障害性のある方法で展開できます。こうすることで、1 台の AAA サーバが利用できなくなっても、SSH などのインタラクティブ管理アクセスが可能になります。

冗長 AAA サーバ ソリューションを設計または実装する場合は、次の点を考慮に入れてください。

1. ネットワーク障害が発生した場合の AAA サーバのアベイラビリティ
2. 地理的に分散した場所への AAA サーバの配置
3. 定常状態と障害状態での個々の AAA サーバへの負荷
4. ネットワーク アクセス サーバと AAA サーバの間のネットワーク遅延
5. AAA サーバ データベースの同期

詳細は、『Access Control Server の展開』を参照してください。

Simple Network Management Protocol の強化

このセクションでは、IOS-XEデバイス内でのSNMPの展開を保護するために使用できるいくつかの方法について説明します。ネットワーク データと、このデータを送信するネットワーク デバイスの両方の機密性、整合性、およびアベイラビリティを保護するには、SNMP を適切に保護することが重要です。SNMP からは、ネットワーク デバイスの状態に関する豊富な情報が提供されます。この情報は、ネットワークに対する攻撃を実行するためにこのデータを利用する悪意のあるユーザから保護できます。

SNMP コミュニティ ストリング

コミュニティストリングは、デバイス上のSNMPデータへの読み取り専用アクセスと読み取り/書き込みアクセスの両方を制限するためにIOS-XEデバイスに適用されるパスワードです。これらのコミュニティストリングは、すべてのパスワードと同様に、単純なものではないように慎重に選択できます。コミュニティストリングは、ネットワークセキュリティポリシーに従って定期的に変更できます。

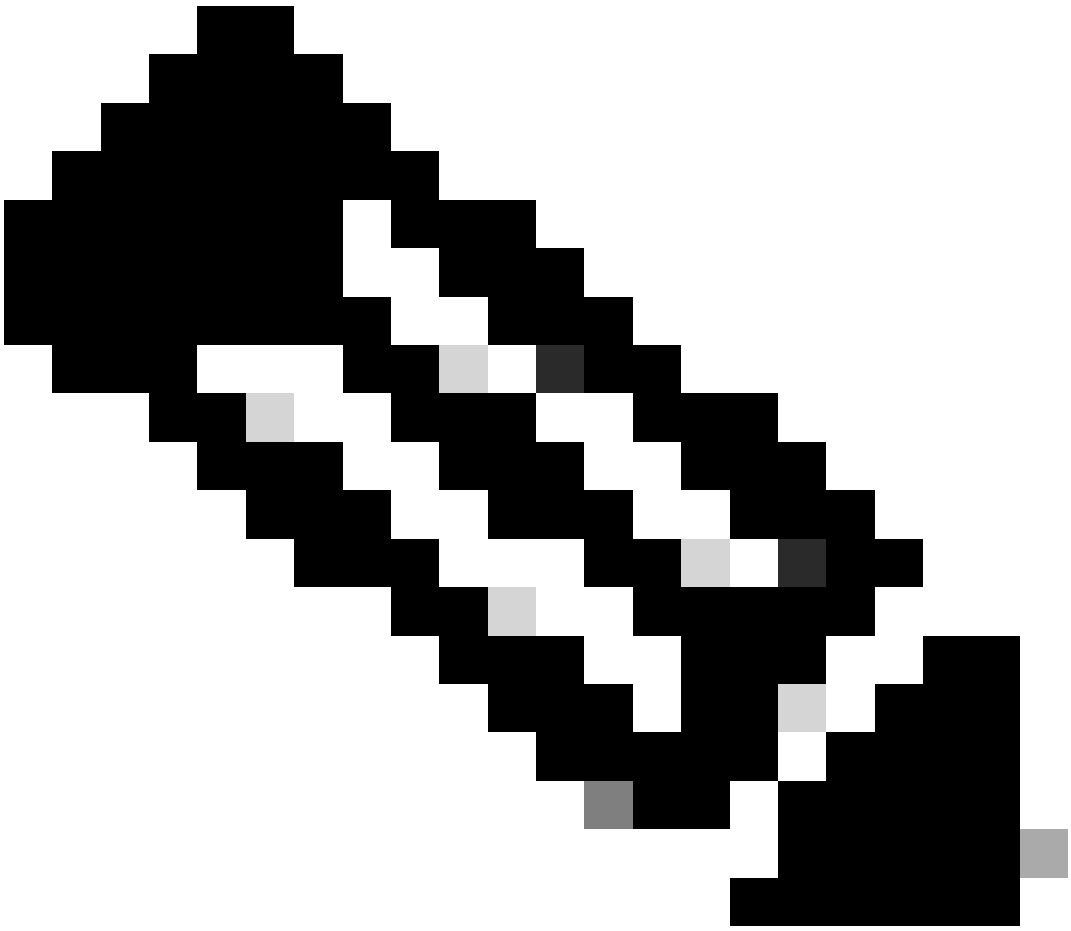
たとえば、ネットワーク管理者がロールを変更したり、会社を退職したりすると、文字列が変更されることがあります。

次の設定では、読み取り専用のコミュニティ ストリングを READONLY、読み書きのコミュニテ

ィ ストリングを READWRITE としています。

snmp-server community読み取り専用RO

snmpサーバコミュニティREADWRITE RW

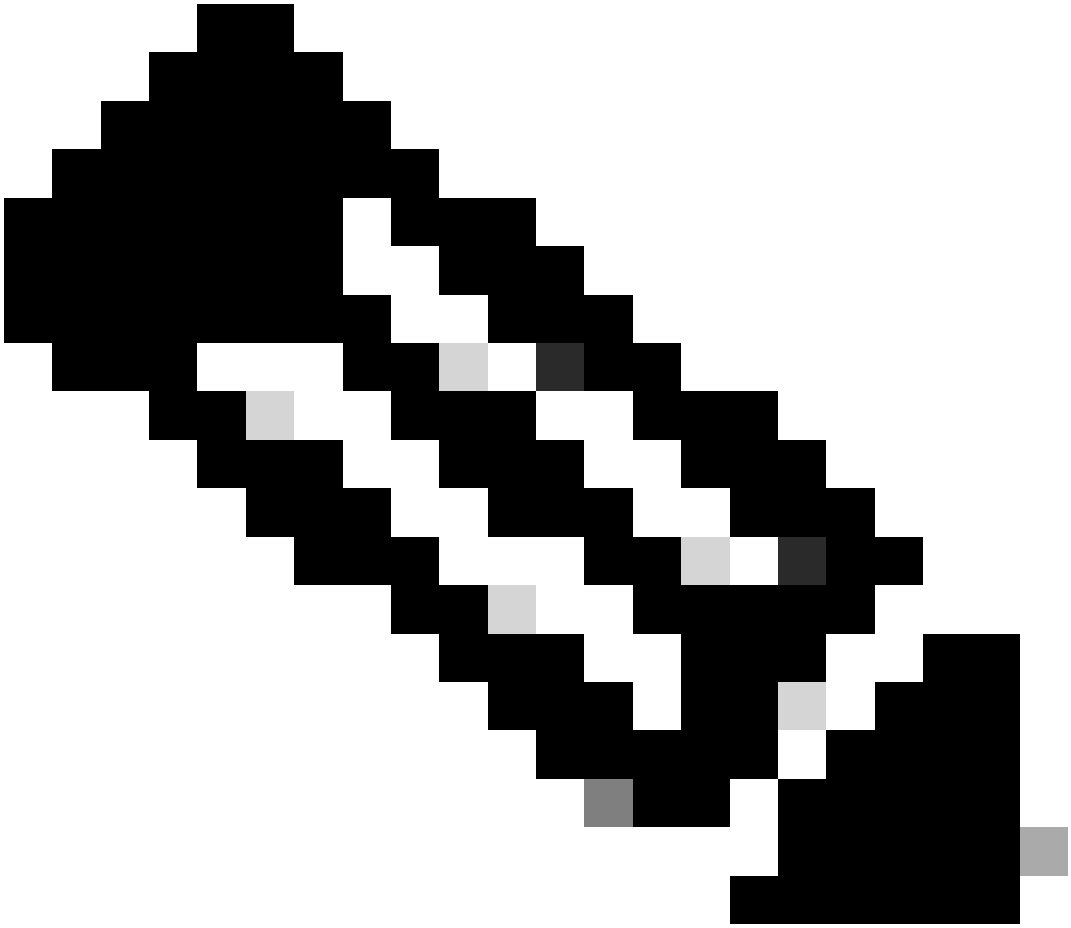


注：上記のコミュニティストリングの例は、これらのストリングの使用法をわかりやすく説明するために選択されたものです。実稼働環境では、コミュニティストリングは慎重に選択でき、アルファベット、数字、および英数字以外の一連の記号で構成されている場合があります。ありふれた文字列ではないパスワードの選択に関する詳細は、『堅牢なパスワードを作成する上での推奨事項』を参照してください。

SNMP コミュニティ ストリングと ACL

コミュニティストリングに加えて、SNMPアクセスを特定の送信元IPアドレスのグループにさらに制限するACLを適用できます。この設定は、SNMPの読み取り専用アクセスを192.168.100.0/24アドレス空間に存在するエンドホストデバイスに制限し、SNMPの書き込み可

能アクセスを192.168.100.1のエンドホストデバイスのみに制限します。



> 注：これらのACLで許可されるデバイスが要求されたSNMP情報にアクセスするには、適切なコミュニティストリングが必要です。

---

access-list 98 permit 192.168.100.0 0.0.0.255

access-list 99 permit 192.168.100.1

snmp-server community READONLY RO 98

snmpサーバコミュニティREADWRITE RW 99

この機能の詳細については、『Cisco IOS XEネットワーク管理コマンドリファレンス』の「snmp-server community」を参照してください。

インフラストラクチャ ACL

インフラストラクチャACL(iACL)を展開すると、信頼できるIPアドレスを持つエンドホストだけがIOS-XEデバイスにSNMPトラフィックを送信できます。iACLには、UDPポート161で不正なSNMPパケットを拒否するポリシーを含めることができます。

iACLの使用方法についての詳細は、このドキュメントの「インフラストラクチャACLによるネットワークアクセス制限」セクションを参照してください。

SNMP ビュー

SNMP ビューは、特定の SNMP MIB へのアクセスを許可または拒否できるセキュリティ機能です。ビューを作成してsnmp-server community community string viewグローバルコンフィギュレーションコマンドでコミュニティストリングに適用すると、MIBデータにアクセスする場合、そのビューに定義された権限に制限されます。必要に応じて、SNMP のユーザを必要なデータに制限するためにビューを使用することを推奨いたします。

次の設定例では、コミュニティ ストリング LIMITED が設定された SNMP アクセスを、system グループ内にある MIB データに制限しています。

snmp-server view <view_name> <mib_view_family_name> [include/exclude]

snmp-server community <community_string>view <view_name> RO

詳細は、『SNMP サポートの設定』を参照してください。

SNMP バージョン 3

SNMPバージョン3(SNMPv3)は、RFC3410、RFC3411、RFC3412、RFC3413、RFC3414、およびRFC3415で定義されており、相互運用可能なネットワーク管理用の標準ベースのプロトコルです。SNMPv3 では、ネットワーク上のパケットが認証され、オプションで暗号化されることから、デバイスへのアクセスが保護されます。SNMPv3 がサポートされている場合、SNMP を展開する際のセキュリティがより一層強化されます。SNMPv3 には、次の 3 つの主要設定オプションがあります。

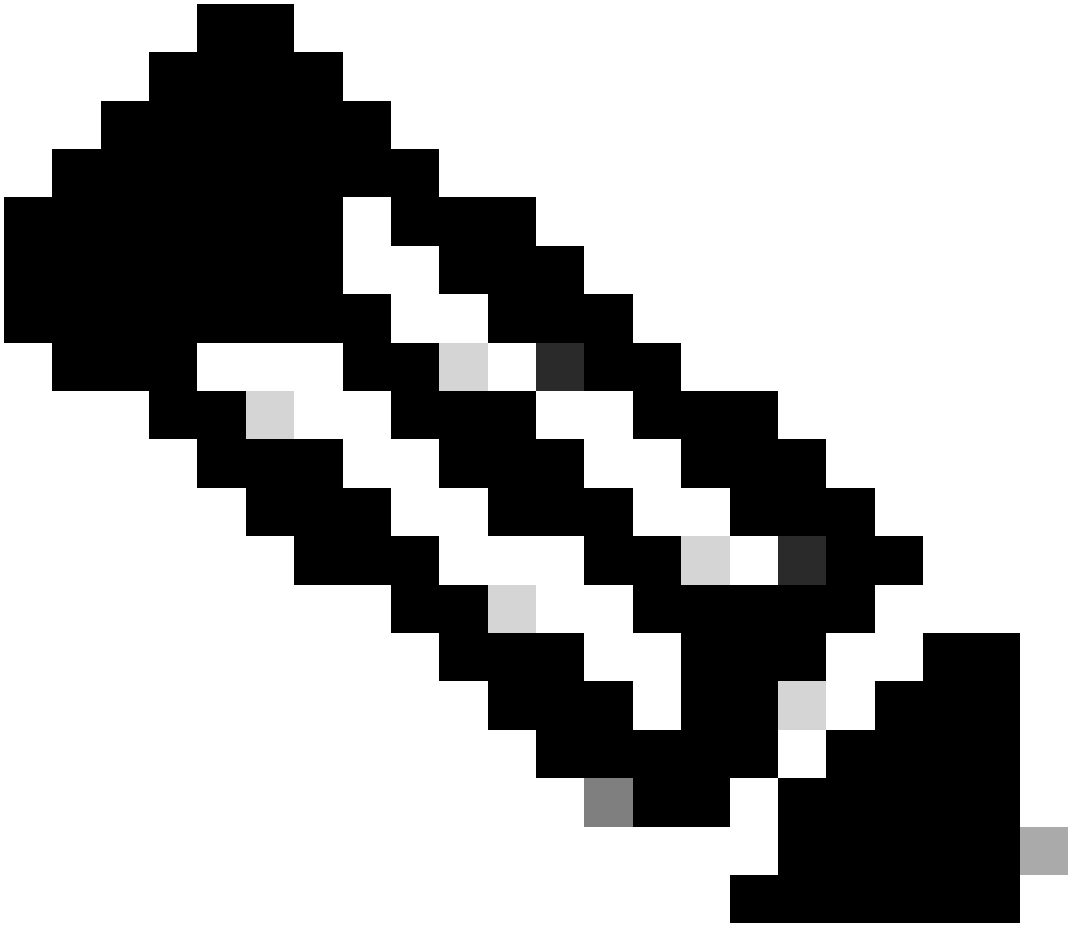
1. no auth：このモードでは、SNMPパケットの認証や暗号化は不要です。
2. auth：このモードでは、SNMPパケットの認証は必要ですが、暗号化は不要です。
3. priv：このモードでは、各SNMPパケットの認証（プライバシー）と暗号化（プライバシー）が必要です。

SNMPv3セキュリティメカニズムを使用してSNMPパケットを処理するには、正規のエンジンIDが存在している必要があります。デフォルトでは、エンジンIDはローカルに生成されます。エンジン ID を表示するには、次の例で示すように show snmp engineID コマンドを使用します。

router#show snmp engineID

ローカルSNMPエンジンID:800000090300000152BD35496

リモートエンジンID IPアドレスポート



注：engineIDを変更した場合は、すべてのSNMPユーザアカウントを再設定する必要があります。

次に、SNMPv3 グループの設定を行います。次のコマンドでは、SNMPサーバグループAUTHGROUPのSNMPv3対応Cisco IOS XEデバイスを設定していますが、authキーワードの使用により認証のみがイネーブルにされています。

snmp-serverグループAUTHGROUP v3認証

このコマンドは、SNMPサーバグループを持つSNMPv3対応Cisco IOS XEデバイスを設定します。

PRIVGROUPに追加し、privキーワードを使用してこのグループの認証と暗号化をイネーブルにします。

snmpサーバグループPRIVGROUP v3 priv

次のコマンドでは、SNMPv3 ユーザ snmpv3user に、MD5 認証パスワード authpassword と 3DES 暗号化パスワード privpassword を設定しています。

snmp-serverユーザsnmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des privpassword

snmp-server userコンフィギュレーションコマンドは、RFC 3414の規定に従って、デバイスのコンフィギュレーション出力には表示されないことに注意してください。そのため、ユーザパスワードはコンフィギュレーションには表示されません。設定されたユーザを表示するには、次の例で示すように、show snmp user コマンドを入力します。

router#show snmp user

ユーザ名：snmpv3ユーザエンジンID:800000090300000152BD35496

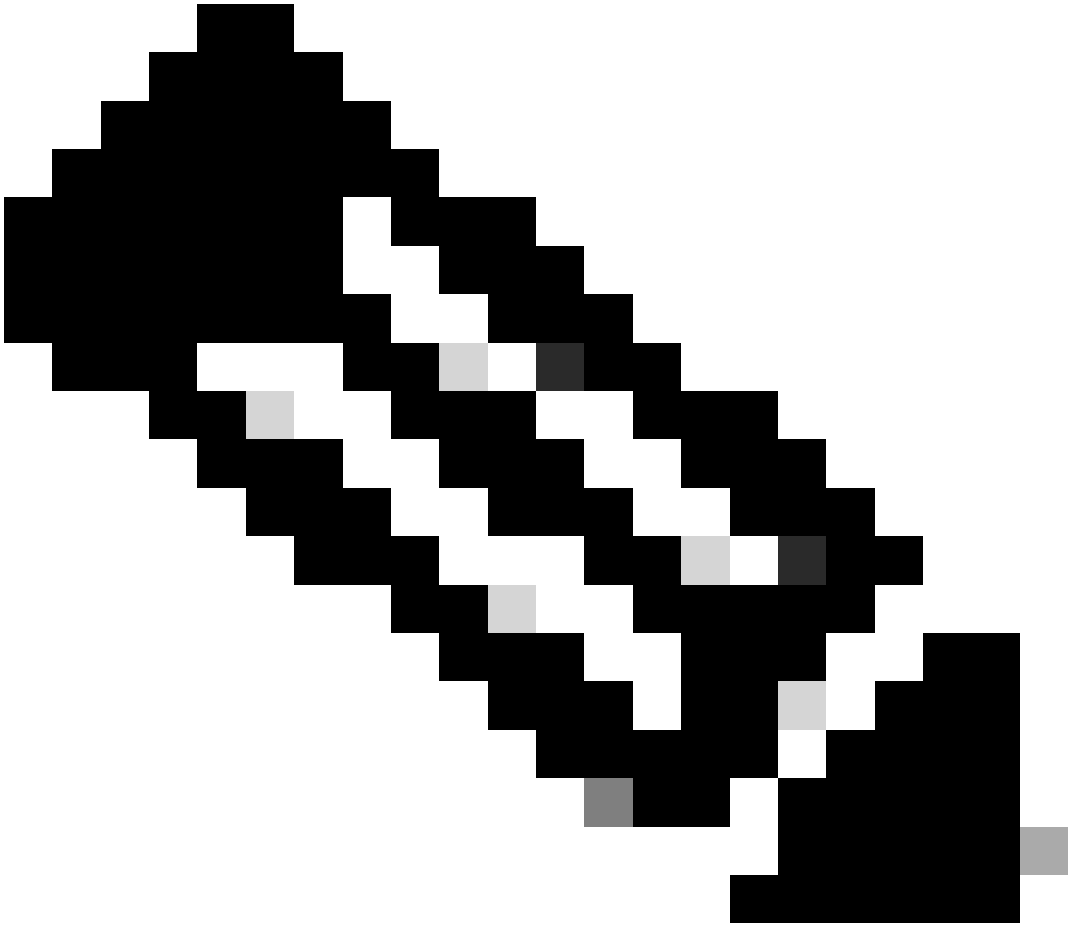
storage-type: nonvolatile active

Authentication Protocol: MD5
プライバシープロトコル：3DES
グループ名：PRIVGROUP

この機能についての詳細は、『SNMP サポートの設定』を参照してください。

管理プレーン保護

Cisco IOS XEソフトウェアの管理プレーン保護(MPP)機能を使用すると、デバイスでSNMPトラフィックを終端できるインターフェイスが制限されるため、SNMPを保護できます。管理者は MPP 機能を使用して、1 つ以上のインターフェイスを管理インターフェイスとして指定できます。管理トラフィックは、これらの管理インターフェイスを経由してのみデバイスに入ることが許可されます。MPP をイネーブルにすると、指定された管理インターフェイス以外のインターフェイスでは、そのデバイス宛のネットワーク管理トラフィックは許可されません。



注:MPPはCPPr機能のサブセットであり、CPPrをサポートするバージョンのIOSが必要です。CPPr についての詳細は、『コントロール プレーン保護について』を参照してください。

次の例では、MPP を使用して SNMP と SSH アクセスを FastEthernet 0/0 インターフェイスのみに制限しています。

コントロールプレーンホスト

management-interface FastEthernet0/0 allow ssh snmpコマンドを使用します。

詳細は、『管理プレーン保護機能ガイド』を参照してください。

ロギングのベスト プラクティス

イベントロギングを使用すると、Cisco IOS XEデバイスの動作と、デバイスが導入されているネットワークを可視化できます。Cisco IOS XEソフトウェアには、組織のネットワーク管理と可視

性の目標を達成するのに役立つ柔軟なロギングオプションがいくつか用意されています。

以降のセクションでは、ロギングを適切に活用し、Cisco IOS XEデバイスでのロギングの影響を最小限に抑えるのに役立つ、ロギングの基本的なベストプラクティスについて説明します。

ログの一元的な場所への送信

ロギング情報をリモート syslog サーバに送信することが推奨されます。こうすることで、複数のネットワーク デバイスが関係するネットワーク イベントとセキュリティ イベントの関連付けや監査をより効果的に実行できるようになります。syslogメッセージはUDPによってクリアテキストで信頼性なく送信されることに注意してください。このため、ネットワークが管理トラフィックに提供する保護（暗号化やアウトオブバンドアクセスなど）を拡張して、syslogトラフィックを含めることができます。

次の設定例では、ロギング情報をリモートsyslogサーバに送信するようにCisco IOS XEデバイスを設定しています。

logging host <ipアドレス>

ログの関連付けについての詳細は、『ファイアウォールとIOS XEルータsyslogイベントを使用したインシデントの識別』を参照してください。

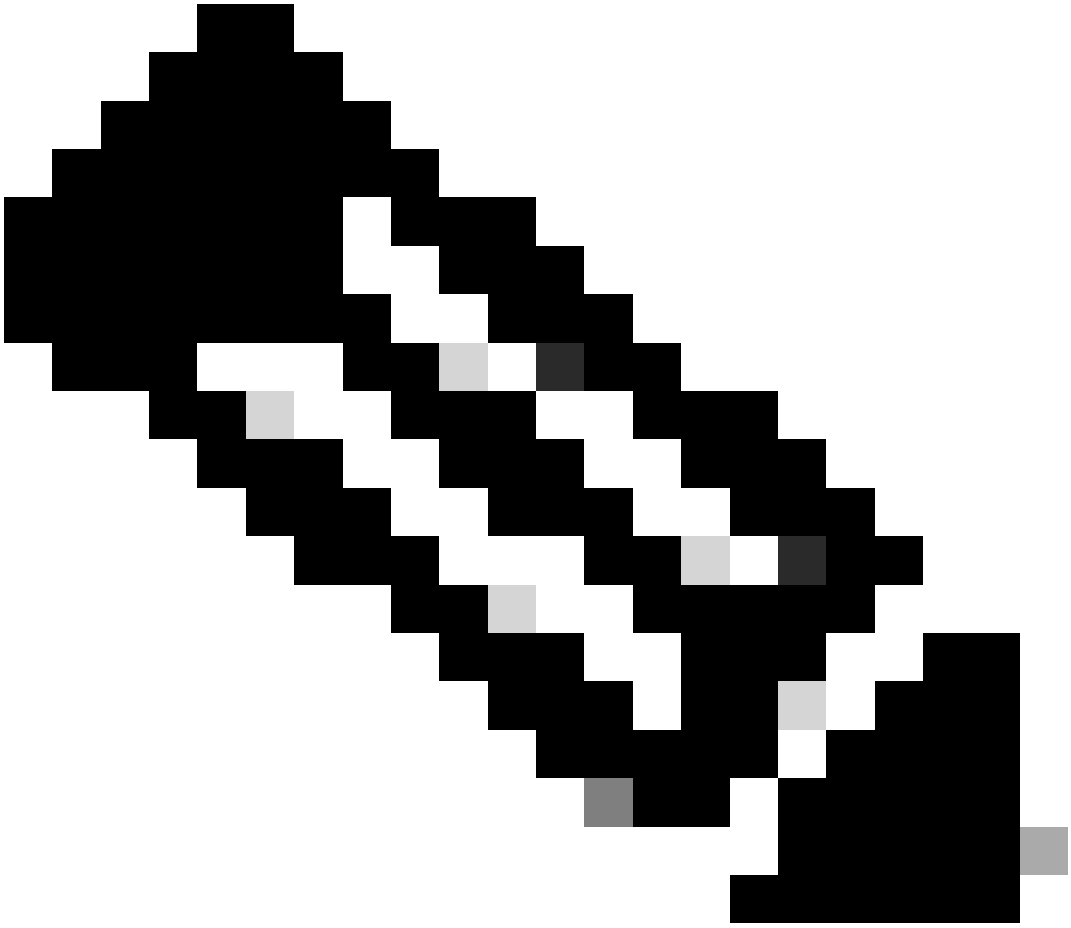
ローカル不揮発性ストレージ（ATAディスク）へのロギング機能を使用すると、システムロギングメッセージをAdvanced Technology Attachment(ATA)フラッシュディスクに保存できます。ATA ドライブに保存されたメッセージは、ルータが再起動した後も残ります。

次の設定行では、ATAフラッシュ(disk0)のsyslogディレクトリへのロギングメッセージを134,217,728バイト(128 MB)に設定し、ファイルサイズを16,384バイトに指定しています。

logging buffered.

logging persistent url disk0:/syslog size 134217728 filesize 16384

ロギングメッセージがATAディスクのファイルに書き込まれる前に、Cisco IOS XEソフトウェアは十分なディスク領域があるかどうかを確認します。十分なディスク スペースがない場合、ロギング メッセージの最も古いファイル（タイムスタンプによる）が削除され、現在のファイルが保存されます。ファイル名の形式はlog_month:day:year::timeです。



注:ATAフラッシュドライブのディスク領域は限られているため、保存データが過度に増加しないように保持する必要があります。

次に、メンテナンス手順の一部としてルータATAフラッシュ ディスクからFTPサーバ 192.168.1.129の外部ディスクにロギング メッセージをコピーする例を示します。

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

この機能の詳細については、『ローカル不揮発性ストレージ（ATAディスク）へのロギング』を参照してください。

ログ レベル

Cisco IOS XEデバイスによって生成される各ログメッセージには、レベル0（緊急）からレベル7（デバッグ）までの8つの重大度のいずれか1つが割り当てられます。特に必要ない限り、レベル 7 でのロギングは行わないことをお勧めします。レベル 7 でロギングを行うと、デバイスの CPU 負荷が上昇し、その結果、デバイスとネットワークが不安定になることがあります。

どのロギング メッセージをリモート syslog サーバに送信するかを指定するには、グローバル コンフィギュレーション コマンド logging trap level を使用します。level に指定する数値を下限とする重大度のメッセージが送信されます。バッファにログを記録するには、logging buffered level コマンドを使用します。

次の設定例では、リモート syslog サーバとローカル ログ バッファに送信するログ メッセージを重大度 6（informational）から 0（emergencies）に制限しています。

ロギングトラップ6

ロギングバッファ6

コンソールまたはモニタ セッションへのログ送信の禁止

Cisco IOS XEソフトウェアでは、ログメッセージをモニタセッションやコンソールに送信することが可能です。モニタセッションは、EXECコマンドterminal monitorが発行されたインタラクティブ管理セッションです。ただし、これはIOS-XEデバイスのCPU負荷を高める可能性があるため、推奨されません。その代わりに、ロギング情報をローカル ログ バッファに送信することが推奨されます。バッファは show logging コマンドを使用して表示できます。

コンソールやモニタ セッションへのロギングをディセーブルにするには、グローバル コンフィギュレーション コマンドの no logging console と no logging monitor を使用します。次の設定例は、これらのコマンドの使用法を示しています。

no logging console

no logging monitor

グローバル設定コマンドの詳細については、『Cisco IOS XEネットワーク管理コマンドリファレンス』を参照してください。

バッファ ロギングの使用

Cisco IOS XEソフトウェアでは、ローカルに生成されたログメッセージを管理者が表示できるように、ローカルログバッファの使用がサポートされています。コンソールやモニタ セッションにログを送信するのではなく、ログをバッファに記録することを強く推奨いたします。

バッファ ロギングの設定に関連するオプションは、ロギング バッファ サイズと、バッファに保管されるメッセージの重大度の 2 つがあります。ロギング バッファのサイズを設定するには、グローバル コンフィギュレーション コマンド logging buffered size を使用します。バッファに記録する最低の重大度を設定するには、logging buffered severity コマンドを使用します。管理者は show logging EXEC コマンドを使用して、ロギング バッファの内容を表示できます。

次の設定例では、ロギング バッファのサイズを 16384 バイト、重大度を 6（informational）に設定しています。これにより、重大度 0（emergencies）から 6（informational）までのメッセージが保管されます。

logging buffered 16384 6（バッファリングされたログ）

バッファロギングについての詳細は、『Cisco IOS XEメッセージ表示宛先デバイスの設定』を参照してください。

ロギングの発信元インターフェイスの設定

ログ メッセージの収集と確認を行う際の一貫性を高めるため、ロギングの発信元インターフェイスを静的に設定することを推奨いたします。

logging source-interfaceインターフェイスコマンドを使用して、ロギングの発信元インターフェイスを静的に設定することで、個々のCiscoIOSデバイスから送信されるすべてのロギングメッセージには、それぞれ同じIPアドレスが表示されるようになります。さらに安定性を高めるために、ロギングの発信元としてループバック インターフェイスを使用することをお勧めします。

次の設定例では、logging source-interface interface グローバル コンフィギュレーション コマンドを使用して、すべてのログ メッセージでループバック 0 インターフェイスの IP アドレスが使用されるように指定しています。

logging source-interface Loopback 0

詳細については、『Cisco IOS XE Embedded Syslog Manager』を参照してください。

ロギングのタイムスタンプの設定

ロギングのタイムスタンプを設定すると、複数のネットワーク デバイスが関係するイベントの関連付けに役立ちます。ロギング データを関連付けられるように、正確で一貫したロギング タイムスタンプが設定されていることが重要です。ロギングのタイムスタンプは、ミリ秒単位の精度で日付と時刻を含め、デバイスで使用されているタイムゾーンを含めるように設定できます。

次の例では、ロギング タイムスタンプを Coordinated Universal Time（UTC; 世界標準時）ゾーンのミリ秒単位で設定しています。

service timestamps log datetime msec show-timezone

ログの時刻を UTC 以外のタイム ゾーンにする場合は、ローカルのタイム ゾーンを指定して、生成されたログ メッセージにその情報が表示されるように設定できます。次の例では、Pacific Standard Time（PST; 太平洋標準時）にデバイスを設定しています。

clock timezone PST -8

service timestamps log datetime msec localtime show-timezone

Cisco IOS XEソフトウェアの構成管理

Cisco IOS XEソフトウェアには、Cisco IOS XEデバイスで構成管理の形式を有効にできる機能がいくつか含まれています。このような機能には、コンフィギュレーションのアーカイブ、前のコンフィギュレーション バージョンへのロールバック、詳細なコンフィギュレーション変更ログの作成などがあります。

設定の置換と設定のロールバック

Cisco IOS XEソフトウェアリリース16.6.4以降では、コンフィギュレーションの置換機能とコンフィギュレーションのロールバック機能を使用して、Cisco IOS XEデバイスのコンフィギュレーションをデバイスにアーカイブできます。このアーカイブに手動または自動で保存されたコンフィギュレーションは、configure replace filename コマンドを使用して、現在の実行コンフィギュレーションを置き換えることができます。これは、copy filename running-config コマンドとは異なった働きです。copy コマンドを実行するとマージが行われるのに対して、configure replace filename コマンドを使用すると、実行コンフィギュレーションが置き換えられます。

ネットワーク内のすべてのCisco IOS XEデバイスでこの機能を有効にすることを推奨します。イネーブルにすると、archive config 特権 EXEC コマンドを使用して、現在の実行コンフィギュレーションをアーカイブに追加できます。アーカイブに追加されたコンフィギュレーションは、show archive EXEC コマンドを使用して表示できます。

次の例では、コンフィギュレーションを自動的にアーカイブに追加する設定を示しています。また、このコマンドはCisco IOS XEデバイスに対し、アーカイブされた設定をarchived-config-Nという名前のファイルとしてdisk0：ファイルシステムに保存し、最大14個のバックアップを保持して、アーカイブを1日に1回（1440分）、管理者がwrite memory EXECコマンドを発行したときに実行するよう指示します。

アーカイブ

パスdisk0:archived-config

最大14

時間帯1440

コンフィギュレーション アーカイブ機能では最大 14 個のバックアップ コンフィギュレーションを保存できますが、スペースの要件を考慮した上で maximum コマンドを使用することを推奨いたします。

コンフィギュレーション変更の排他的アクセス

Cisco IOS XEソフトウェアリリース16.6.4では、コンフィギュレーション変更の排他的アクセス機能が追加され、Cisco IOS XEデバイスのコンフィギュレーション変更を行う管理者は常に1人だけになります。この機能により、関連するコンフィギュレーション コンポーネントが同時に変更されることによる、望ましくない影響をなくすことができます。この機能を設定するには、グローバルコンフィギュレーションコマンドconfiguration mode exclusiveモードを使用します。動作モードにはautoとmanualの2つがあります。auto モードでは、管理者が configure terminal EXEC コマンドを発行すると、コンフィギュレーションが自動的にロックされます。manual モードでは、コンフィギュレーション モードに入る際に管理者が configure terminal lock コマンドを使用して、コンフィギュレーションをロックします。

次の例では、この機能を使用してコンフィギュレーションを自動的にロックする設定を示してます。

排他コンフィギュレーションモード

デジタル署名付き Cisco ソフトウェアの識別

Cisco IOS XEソフトウェアリリース16.1以降で追加されたデジタル署名付きシスコソフトウェア機能は、セキュアな非対称（公開キー）暗号化を使用して、デジタル署名付きで信頼できるCisco IOS XEソフトウェアの使用を促進します。

デジタル署名されたイメージは、自身の暗号化された（秘密キーを使用して）ハッシュを運びます。チェックでは、デバイスは対応する公開キーで、キーの中にあるキーからハッシュを復号し、イメージの自身のハッシュも計算します。復号されたハッシュが計算されたイメージのハッシュと一致すると、イメージは改ざんされておらず信頼できます。

デジタル署名されたシスコのソフトウェア キーは、キーの種類やバージョンで識別されます。使用できるキーの種類は、特殊、実稼働、またはロール オーバーです。実稼働および特殊な種類のキーは、キーがいつ取り消されたり置き換わったりしても、アルファベット順で増分する関連づけられたキー バージョンを持ちます。デジタル署名付きシスコソフトウェア機能を使用すると、ROMMONイメージと通常のCisco IOS XEイメージの両方が特殊キーまたは実稼働キーで署名されます。ROMMON イメージはアップグレード可能で、ロードされる特殊または実稼働イメージと同じキーで署名される必要があります。

このコマンドは、デバイスのキーストア内のキーを使用して、フラッシュ内のイメージisr4300-universalk9.16.06.04.SPA.binの整合性を確認します。

show software authenticity file bootflash:isr4300-universalk9.16.06.04.SPA.bin（入手可能）

この機能についての詳細は、『デジタル署名付き Cisco ソフトウェア』を参照してください。

その後、新しいイメージ(isr4300-universalk9.16.10.03.SPA.bin)をフラッシュにコピーしてロードすると、新しく追加された特殊キーを使用してイメージの署名が検証されます

copy /verify tftp://<server_ip>/isr4300-universalk9.16.10.03.SPA.bin flash:

設定変更通知とロギング

Cisco IOS XEソフトウェアリリース16.6.4で追加されたConfiguration Change Notification and Logging機能を使用すると、Cisco IOS XEデバイスに加えられた設定変更をログに記録できます。ログはCisco IOS XEデバイスで保持され、変更を行ったユーザの情報、入力したコンフィギュレーションコマンド、および変更を行った時刻が記録されます。この機能をイネーブルにするには、logging enable 設定変更ロガー コンフィギュレーション モード コマンドを使用します。デフォルトの設定を改善するには、オプションコマンドのhide keysおよびlogging sizeエントリを使用します。これらのコマンドを使用すると、パスワードデータをログに記録できなくなり、変更ログのサイズが増加します。

Cisco IOS XEデバイスの構成変更履歴を容易に理解できるようにするため、この機能を有効にすることを推奨します。さらに、コンフィギュレーションの変更時に syslog メッセージが生成されるように、notify syslog コンフィギュレーション コマンドを使用することを推奨します。

アーカイブ

ログ設定

ロギングの有効化

ログサイズ200

隠しキー

syslogの通知

コンフィギュレーション変更通知とロギング機能をイネーブルにすると、特権 EXEC コマンド show archive log config all を使用して、コンフィギュレーション ログを表示できます。

コントロール プレーン

コントロール プレーン機能は、発信元から宛先へデータを移動するために、ネットワーク デバイス間でやりとりされるプロトコルとプロセスで構成されます。これには、ボーダー ゲートウェイ プロトコルなどのルーティング プロトコルや、ICMP および Resource Reservation Protocol（RSVP; リソース予約プロトコル）のようなプロトコルが含まれます。

管理プレーンおよびデータ プレーンでのイベントによって、コントロール プレーンに悪影響が及ばないようにすることが重要です。DoS攻撃などのデータプレーンイベントがコントロールプレーンに影響を与えると、ネットワーク全体が不安定になる可能性があります。Cisco IOS XEソフトウェアの機能と設定に関するこの情報は、コントロールプレーンの復元力の確保に役立ちます。

コントロール プレーン全般の強化

管理プレーンとデータ プレーンの維持と稼働は、コントロール プレーンにかかっているので、ネットワーク デバイスのコントロール プレーンを保護することは重要です。セキュリティ事象の発生中にコントロール プレーンが不安定になると、ネットワークの安定性を回復できないおそれがあります。

多くの場合、インターフェイスで特定の種類のメッセージの送受信をディセーブルにすることで、不要なパケットを処理するために必要な CPU 負荷を最小にできます。

IP ICMP リダイレクト

同じインターフェイスでパケットを送受信する際に、ルータでは ICMP リダイレクト メッセージが生成される場合があります。この場合、ルータはパケットを転送し、元のパケットの送信者には ICMP リダイレクト メッセージを送信します。この動作により、送信者はそのルータをバイパスして、後続パケットを宛先（または宛先により近いルータ）に直接転送できます。正常に機能している IP ネットワークでは、ルータは自分のローカル サブネット上のホストに対してだけリダイレクトを送信します。つまり、ICMPリダイレクトはレイヤ3境界を越えることはできません。

ICMP リダイレクト メッセージには、ホスト アドレスのリダイレクトとサブネット全体のリダイレクトという 2 つのタイプがあります。悪意のあるユーザがルータに連続してパケットを送信し、これにより強制的にルータを ICMP リダイレクト メッセージに対応させて、CPU とルータのパフォーマンスに悪影響を及ぼすことによって、ICMP リダイレクトを送信するルータの機能を悪用する可能性があります。ルータが ICMP リダイレクトを送信しないようにするには、no ip redirects インターフェイス コンフィギュレーション コマンドを使用します。

ICMP 到達不能

インターフェイス アクセス リストによるフィルタリングを行うと、フィルタリングされたトラフィックの発信元には ICMP 到達不能メッセージが送信されます。これらのメッセージの生成により、デバイスの CPU 使用率が増加することがあります。Cisco IOS XEソフトウェアでは、ICMP到達不能メッセージの生成は、デフォルトで500ミリ秒ごとに1パケットに制限されています。ICMP 到達不能メッセージの生成を無効にするには、インターフェイス コンフィギュレーション コマンド no ip unreachables を使用します。ICMP 到達不能レート制限をデフォルト設定から変更するには、グローバル コンフィギュレーション コマンド icmp rate-limit unreachable interval-in-ms を使用します。

プロキシ ARP

プロキシ ARP は、あるデバイス（通常はルータ）が、別のデバイスに宛てられた ARP 要求に応答する技法です。ルータは、そのIDを偽装することで、実際の宛先にパケットをルーティングする責任を引き受けます。プロキシ ARP を使用すると、ルーティングやデフォルト ゲートウェイを設定しなくても、サブネット上のマシンがリモートのサブネットに容易に到達できるようになります。プロキシ ARP は、RFC 1027 で定義されています。

プロキシ ARP を使用するには、いくつかの短所があります。プロキシ ARP を使用すると、ネットワーク セグメント上の ARP トラフィック、およびリソース枯渇攻撃や中間者（man-in-the-middle）攻撃が増加する可能性があります。プロキシ ARP では、プロキシ処理されたそれぞれの ARP 要求が少量のメモリを消費するので、リソース枯渇攻撃が誘発されます。攻撃者は ARP 要求を大量に送信することによって、利用可能なメモリを枯渇させることができます。

中間者攻撃では、ネットワーク上のホストがルータの MAC アドレスをスプーフィングすることによって、無警戒なホストが攻撃者にトラフィックを送信することが可能になります。プロキシ ARP をディセーブルにするには、インターフェイス コンフィギュレーション コマンド no ip proxy-arp を使用します。

この機能についての詳細は、『プロキシARPのイネーブル化とディセーブル化』を参照してください。

NTP制御メッセージ

NTP制御メッセージクエリは、より優れたNMが作成および使用される前にネットワーク管理(NM)機能を支援するNTPの機能です。組織でNM機能にNTPを使用している場合を除き、ネットワークセキュリティのベストプラクティスは、それらすべてを完全に無効にすることです。これらを使用している場合は、ファイアウォールまたはその他の外部デバイスによってブロックされている内部ネットワーク専用タイプのサービスである可能性があります。IOS-XRおよびNX-

OSではこれらのバージョンがサポートされていないため、標準のIOSおよびIOS-XEバージョン以外のすべてのバージョンから削除されました。

この機能を無効にした場合、コマンドは

```
Router (config)# no ntp allow mode control
```

このコマンドを実行すると、running-configにno ntp allow mode control 0と表示されます。これにより、デバイスのNTP制御メッセージが無効になり、デバイスが攻撃から保護されます。

コントロール プレーン トラフィックの CPU への影響の制限

コントロール プレーンの保護は非常に重要です。データ トラフィックと管理トラフィックが滞ればアプリケーション パフォーマンスとエンドユーザ エクスペリエンスが損なわれる可能性があるので、管理プレーンとデータ プレーンの維持と稼働はコントロール プレーンの持続性にかかっていると言えます。

コントロール プレーン トラフィックについて

Cisco IOS XEデバイスのコントロールプレーンを適切に保護するには、CPUによってプロセススイッチングされるトラフィックのタイプを理解することが不可欠です。プロセス スイッチングされるトラフィックは、通常、2 種類のトラフィックで構成されます。最初のタイプのトラフィックはCisco IOS XEデバイス宛てであり、Cisco IOS XEデバイスのCPUで直接処理する必要があります。このトラフィックは、受信隣接関係トラフィックカテゴリで構成されます。このトラフィックには、次のルータホップがそのデバイス自体であるCisco Express Forwarding(CEF)テーブル内のエントリが含まれています。これは、show ip cef CLI出力のreceiveという用語で示されます。これは、インターフェイスIPアドレス、マルチキャストアドレス空間、ブロードキャストアドレス空間など、Cisco IOS XEデバイスのCPUによる直接処理が必要なIPアドレスの場合に表示されます。

CPUで処理される2つ目のタイプのトラフィックは、データプレーントラフィック（Cisco IOS XEデバイス以外の宛先を持つトラフィック）です。このトラフィックには、CPUによる特別な処理が必要です。データプレーントラフィックに影響を与えるCPUの完全なリストではありませんが、これらのタイプのトラフィックはプロセススイッチングされるため、コントロールプレーンの動作に影響を与える可能性があります。

1. アクセス コントロール リスト ロギング：ACL ロギング トラフィックは、log キーワードが使用された場合の ACE の一致（許可または拒否）によって生成されるあらゆるパケットで構成されます。
2. ユニキャスト リバース パス フォワーディング（ユニキャスト RPF）：ユニキャスト RPF は、ACL とともに使用され、特定のパケットのプロセス スイッチングが行われる可能性があります。
3. IP オプション：オプションが指定された任意の IP パケットは、CPU で処理する必要があります。
4. フラグメンテーション：フラグメンテーションを必要とする任意の IP パケットは、CPU に渡して処理する必要があります。
5. 存続可能時間（TTL）の期限切れ：TTL 値が 1 以下のパケットでは、インターネット制御メ

ッセージ プロトコルの Time Exceeded（ICMP タイプ 11、コード 0）メッセージが送信される必要があります。これにより CPU 処理が発生します。
6. ICMP 到達不能：ルーティング、MTU、またはフィルタリングによって ICMP 到達不能メッセージを発生させるパケットは、CPU で処理されます。
7. ARP 要求を必要とするトラフィック：ARP エントリが存在しない宛先は、CPU での処理が必要です。
8. 非 IP トラフィック：すべての非 IP トラフィックは CPU で処理されます。

次のリストでは、Cisco IOS XEデバイスのCPUで処理されるトラフィックのタイプを判別する方法について詳しく説明します。
9. show ip cef コマンドを実行すると、CEF テーブルに含まれる各 IP プレフィクスのネクストホップ情報が表示されます。すでに説明したように、ネクストホップとしてreceiveを含むエントリは、受信隣接関係と見なされ、トラフィックをCPUに直接送信する必要があることを示します。
10. show interface switching コマンドを実行すると、デバイスでプロセス スイッチングされているパケット数の情報が表示されます。
11. show ip trafficコマンドを実行すると、IPパケットの数に関する情報が表示されます。ローカルな宛先（つまり、受信隣接関係のトラフィック）とオプションが表示され、それらのオプションは、マルチキャストアドレス空間に送信されるブロードキャストアドレス空間に送信されるフラグメンテーションを必要とします。
12. 受信隣接関係トラフィックを識別するには、show ip cache flow コマンドを使用します。Cisco IOS XEデバイス宛てのフローの宛先インターフェイス(DstIf)はlocalです。
13. コントロールプレーンポリシングを使用すると、Cisco IOS XEデバイスのコントロールプレーンに到達するトラフィックのタイプとレートを識別できます。コントロール プレーン ポリシングを実行するには、詳細な分類の ACL、ロギング、および show policy-map control-plane コマンドを使用します。

インフラストラクチャ ACL

Infrastructure ACL（iACL; インフラストラクチャ ACL）によって、外部通信をネットワークのデバイスに制限できます。

インフラストラクチャ ACL については、このドキュメントの「インフラストラクチャ ACL によるネットワーク アクセス制限」の項で詳しく説明しています。

iACL を実装して、すべてのネットワーク デバイスのコントロール プレーンを保護することを推奨します。

受信 ACL

rACL は、ルート プロセッサが有害なトラフィックの影響を受ける前に、そのトラフィックからデバイスを保護します。受信 ACL は、それが設定されたデバイスを保護するだけの設計になっており、通過トラフィックには影響を与えません。その結果、例のACLエントリで使用されている宛先IPアドレスanyは、ルータの物理または仮想IPアドレスだけを参照します。受信ACLもネットワークセキュリティのベストプラクティスと考えられており、長期に渡って優れたネットワークセキュリティを付加すると考えることができます。

次に示すのは、192.168.100.0/24 ネットワーク上の信頼できるホストからの SSH (TCP ポート 22) トラフィックを許可するように記述された受信パス ACL です。

---信頼できるホストからデバイスへの SSH を許可します。

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22

---他のすべての発信元から RP への SSH を拒否します。

access-list 151 deny tcp any any eq 22

---セキュリティ ポリシーとコンフィギュレーションに従って、

---設定に従って許可します。

access-list 151 permit ip any any

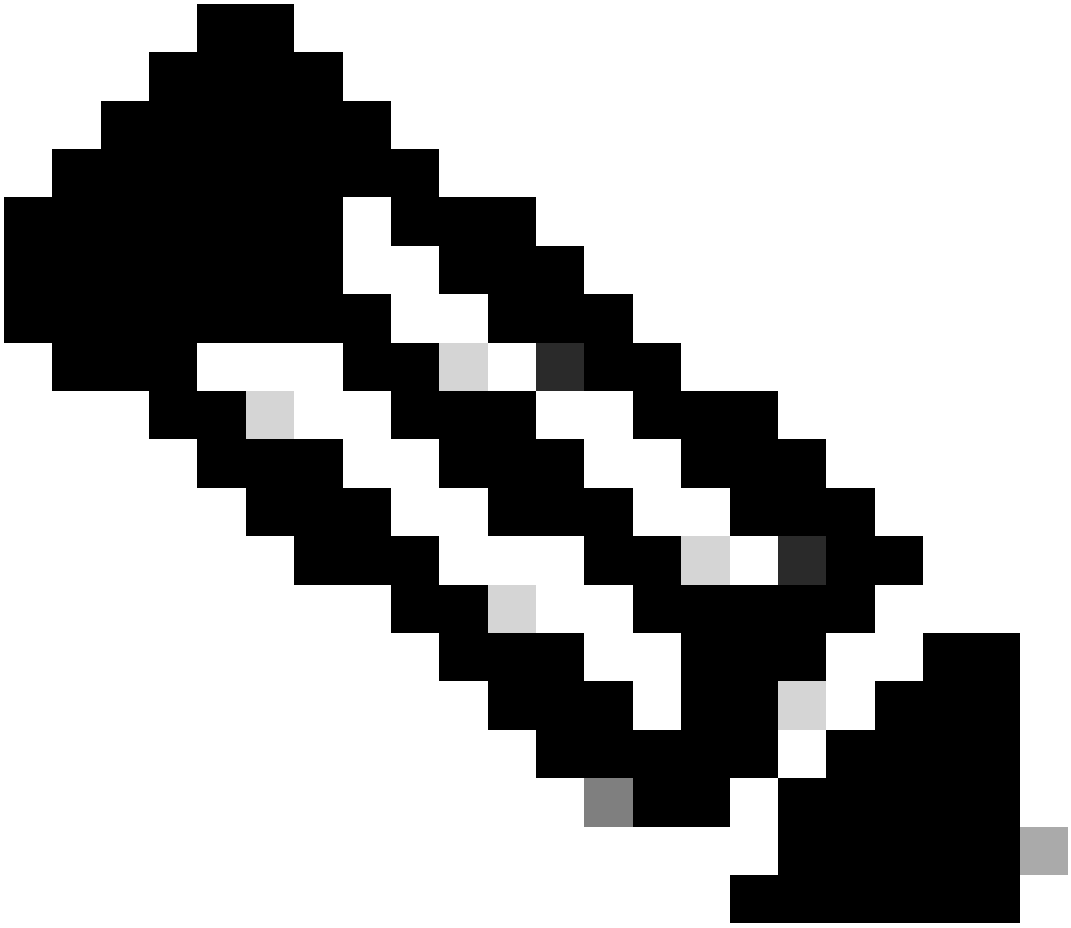
---このアクセス リストを受信パスに適用します。

ip受信アクセスリスト151

デバイスへの正当なトラフィックを識別して許可を与え、望ましくないパケットをすべて拒否するには、『アクセスコントロールリスト』を参照してください。

CoPP

CoPP機能を使用して、インフラストラクチャデバイス宛てのIPパケットを制限することもできます。この例では、信頼できるホストからのSSHトラフィックだけがCisco IOS XEデバイスのCPUに到達できます。



注：不明なIPアドレスや信頼できないIPアドレスからのトラフィックを廃棄することで、動的に割り当てられたIPアドレスを持つホストがCisco IOS XEデバイスに接続するのを防ぐことができます。

---

access-list 152 deny tcp <trusted-addresses> <mask> any eq 22

access-list 152 permit tcp any any eq 22

access-list 152 deny ip any any

class-map match-all COPP-KNOWN-INSIRABLE match access-group 152

policy-map COPP-INPUT-POLICY class COPP-KNOWN-UNWANTED DROP（ポリシーマップCOPP入力ポリシークラスCOPP既知の望ましくないドロップ）

control-plane service-policy input COPP-INPUT-POLICY（コントロールプレーンのサービスポリシー入力COPP-INPUT – ポリシー）

前記の CoPP の例では、ACL エントリの permit アクションに一致する不正なパケットがある場合、このようなパケットはポリシーマップの drop 機能によって廃棄されますが、deny アクションに一致するパケットは、ポリシーマップの drop 機能の影響を受けません。

CoPPは、Cisco IOS XEソフトウェアリリースで使用できます。

CoPP機能の設定と使用法についての詳細は、『コントロールプレーンポリシング』を参照してください。

コントロール プレーン保護

Cisco IOS XEソフトウェアリリース16.6.4で導入されたコントロールプレーン保護(CPPr)を使用すると、Cisco IOS XEデバイスのCPUを宛先とするコントロールプレーントラフィックを制限またはポリシングできます。CPPr は CoPP と同様に、トラフィックを詳細に制限できます。CPPr によって集約コントロール プレーンは、サブインターフェイスと呼ばれる 3 つの個別のコントロール プレーン カテゴリに分割されます。サブインターフェイスが存在するのは、Host、Transit、および CEF-Exception のトラフィック カテゴリです。さらに、CPPr には次のコントロール プレーン保護機能があります。

1. ポートフィルタリング機能：閉じているか受信状態ではない TCP ポートや UDP ポートに送信されるパケットの規制や廃棄を行います。
2. キューしきい値機能：コントロール プレーン IP 入力キューで許可されている指定されたプロトコルのパケット数を制限します。

   CPPr 機能の設定と使用法についての詳細は、『コントロール プレーン保護および『コントロール プレーン保護 (CPPr) について』を参照してください。

ハードウェア レート制限機能

Cisco Catalyst 6500 シリーズ Supervisor Engine 32 および Supervisor Engine 720 では、特殊なネットワーキング シナリオ用にプラットフォーム固有のハードウェアベースのレート制限機能（ HWRL ）がサポートされています。これらのハードウェア レート制限機能は、IPv4、IPv6、ユニキャスト、マルチキャストの DoS 攻撃シナリオに関する詳細な定義済みセットをカバーしており、特殊なケースのレート リミッタと呼ばれています。HWRLは、パケットをCPUで処理する必要のあるさまざまな攻撃からCisco IOS XEデバイスを保護できます。

BGPを固定します

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) は、インターネットのルーティングの基盤です。したがって、標準より厳しい接続要件を設けている組織では、多くの場合、BGP を利用しています。BGPは、そのユビキタス性と、小規模な組織におけるBGP設定の設定および無力化の性質から、多くの場合、攻撃者の標的になります。ただし、BGP 設定のセキュリティ向上に利用できる多くの BGP 固有セキュリティ機能があります。

ここでは、最重要の BGP セキュリティ機能の概要を示します。必要に応じて、コンフィギュレーションの推奨事項も示しています。

TTL ベースのセキュリティ保護

それぞれの IP パケットには、Time To Live（TTL; 存続可能時間）と呼ばれる 1 バイトのフィールドが含まれています。IP パケットがデバイスを通過するごとに、この値は 1 ずつ減ります。開始値はオペレーティング システムによって異なりますが、通常は 64 ~ 255 の間です。TTL 値が 0 に達したパケットは廃棄されます。

Generalized TTL-based Security Mechanism（GTSM）および BGP TTL Security Hack（BTSH）と呼ばれる TTL ベースのセキュリティ保護では、IP パケットの TTL 値を利用することにより、受信 BGP パケットが直接接続されたピアからのものであることが保証されます。この機能には多くの場合、ピアリング ルータからの同調が必要ですが、イネーブルにすると、BGP に対する多くの TCP ベースの攻撃を完全に防ぐことができます。

BGP 用の GTSM をイネーブルにするには、neighbor BGP ルータ コンフィギュレーション コマンドの ttl-security オプションを使用します。次の例は、この機能の設定を示しています。

router bgp <asn>（オプション）

neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> ttl-security hops <hop-count>

BGP パケットが受信されると、TTL 値がチェックされます。TTL 値は、255 から指定の hop-count を差し引いた数値以上である必要があります。

MD5 による BGP ピア認証

MD5 を使用するピア認証により、BGP セッションの一部として送信される各パケットの MD5 ダイジェストが作成されます。ダイジェストの生成には、具体的には、IP および TCP ヘッダー部分、TCP ペイロード、および秘密鍵が使用されます。

作成されたダイジェストは TCP オプション Kind 19 に保存されます。これは、この目的のために RFC 2385 で定義されたオプションです。受信 BGP スピーカはこれと同じアルゴリズムと秘密鍵を使用して、メッセージ ダイジェストを再生成します。受信されたダイジェストと計算されたダイジェストが同じでない場合、パケットは廃棄されます

MD5 によるピア認証を設定するには、neighbor BGP ルータ コンフィギュレーション コマンドの password オプションを使用します。次に、このコマンドの使用法を示します。

router bgp <asn> neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> password <シークレット>

MD5 による BGP ピア認証についての詳細は『ネイバー ルータの認証』を参照してください。

最大プレフィックス数の設定

BGP プレフィクスはルータによりメモリに保持されます。追加のプレフィックス ルータが保持する必要がある場合、多くのメモリをBGPが使用できるようにする必要があります。プロバイダ

一のユーザネットワークに対してデフォルトルートだけを利用する設定など、一部の設定では、すべてのインターネットプレフィクスのサブセットを保存できます。

メモリの枯渇を防ぐために、ピアごとに受け付けるプレフィクスの最大数を設定することが重要です。各 BGP ピアに上限を設定することを推奨いたします。

neighbor maximum-prefix BGPルータコンフィギュレーションコマンドを使用してこの機能を設定する場合、受け入れるプレフィクスの最大数を引数として指定します。この数に達すると、ピアはシャットダウンされます。オプションで、1 ~ 100 の数値を入力することもできます。この数値は最大プレフィクス値に対するパーセンテージを表し、この値に達するとログ メッセージが送信されます。

router bgp <asn> neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>

ピアごとの最大プレフィクスについての詳細は、『BGP 最大プレフィクス機能の設定』を参照してください。

プレフィックス リストによる BGP プレフィックスのフィルタリング

プレフィクス リストを使用すると、BGP を介して送受信される特定のプレフィクスを許可または拒否できます。ネットワークトラフィックが目的のパスを介して送信されるように、可能な限りプレフィックスリストを使用できます。プレフィックスリストは、着信と発信の両方の方向で各eBGPピアに適用できます。

プレフィクス リストを設定すると、送受信されるプレフィクスは、ネットワークのルーティング ポリシーによって具体的に許可されたプレフィクスに制限されます。受信されるプレフィクスが多いためこれが不可能な場合は、既知の不正なプレフィクスを明確にブロックするようにプレフィックスリストを設定できます。このような既知の不正プレフィクスには、未割り当ての IP アドレス レンジや、内部用やテスト用に RFC 3330 で予約済みのネットワークが含まれます。発信プレフィックスリストは、組織がアドバタイズするプレフィクスだけを明確に許可するように設定できます。

次の設定例では、プレフィクス リストを使用して、学習するルートとアドバタイズするルートを制限しています。具体的には、プレフィクス リスト BGP-PL-INBOUND によってデフォルト ルートのみが着信を許可され、BGP-PL-OUTBOUND によってプレフィクス 192.168.2.0/24 のみがアドバタイズを許可されます。

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0を設定します。

ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24を設定します。

router bgp <asn>（オプション）

neighbor <ip-address> prefix-list BGP-PL-INBOUND in

neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out（ネイバー<ipアドレス>プレフィックスリストBGP-PL – アウトバウンド発信）

BGPプレフィクスフィルタリングの詳細は、『プレフィクスベースのアウトバウンドルートフィルタリング』を参照してください。

自律システム パス アクセス リストによる BGP プレフィクスのフィルタリング

BGP 自律システム（AS）パス アクセス リストを使用すると、プレフィクスの AS パス アトリビュートに基づいて、受信されるプレフィクスとアドバタイズされるプレフィクスをフィルタリングできます。これをプレフィクス リストと組み合わせて使用すると、堅牢なフィルタ セットが確立されます。

次の設定例では、AS パス アクセス リストを使用して、着信プレフィクスをリモート AS から発信されたプレフィクスに制限し、発信プレフィクスをローカルの自律システムから発信されたプレフィクスに制限しています。その他すべての自律システムから発信されたプレフィクスはフィルタリングされ、ルーティング テーブルにはインストールされません。

ip as-pathアクセスリスト1 permit

ip as-pathアクセスリスト2 permit

router bgp <asn>（オプション）

neighbor <IPアドレス> remote-AS 65501

neighbor <ip-address> filter-list 1 inコマンド

neighbor <ip-address> filter-list 2 out（ネイバー<ipアドレス> filter-list 2 out）

内部ゲートウェイ プロトコルの保護

ネットワークが適切にトラフィックを転送し、トポロジの変更や障害から回復する能力は、トポロジの正確なビューに依存しています。頻繁にあります。このビューを順番にInterior Gateway Protocol（IGP）を実行できます。デフォルトでは、IGP は動的であり、使用中の特定の IGP と通信するルータの追加を検出します。また、IGP により、ネットワーク リンク障害の発生中に使用可能なルータを検出することもできます。

以降のサブセクションでは、最重要の IGP セキュリティ機能の概要を示しています。

Routing Information Protocol バージョン 2（RIPv2）、Enhanced IGRP（EIGRP）、および OSPF（Open Shortest Path First）について、推奨事項や使用例を交えて説明しています。

MD5 によるルーティング プロトコル認証と検証

ルーティング情報の交換を保護できなければ、攻撃者が不正なルーティング情報をネットワークに持ち込むことが可能になります。ルータ間のルーティングプロトコルでパスワード認証を使用することで、ネットワークのセキュリティを強化できます。ただし、この認証はクリアテキストで送信されるので、攻撃者がこのセキュリティ制御を弱体化させるのは容易である可能性があります。

認証プロセスにMD5ハッシュ機能を追加すると、ルーティング更新にクリアテキストのパスワードが含まれなくなり、ルーティング更新の内容全体が改ざんされにくくなります。ただし、弱いパスワードが選択されている場合は、MD5 認証が力ずくの攻撃や辞書攻撃の影響を受けやすいことに変わりありません。十分にランダム化されたパスワードを使用してください。MD5 認証は、パスワード認証と比べると格段にセキュリティが強化されているので、次の例は MD5 認証に特化しています。IPSec もルーティング プロトコルの検証と保護に使用できますが、次の例ではその使用法については詳しく触れていません。

EIGRP と RIPv2 では、設定の一部としてキー チェーンを使用します。キー チェーンの設定と使用法の詳細は、『鍵』を参照してください。

MD5を使用するEIGRPルータ認証の設定例を次に示します。

キーチェーン

key <キー識別子>

key-string <パスワード>

interface <インターフェイス> ip authentication mode eigrp <as-number> md5

ip authentication key-chain eigrp <as番号> <キー名>

RIPv2 用の MD5 ルータ認証の設定例を次に示します。RIPv1 では認証はサポートされていません。

キーチェーン

key <キー識別子>

key-string <パスワード>

interface <interface> ip rip authentication mode md5

ip rip authentication key-chain <キー名>

これは、MD5を使用するOSPFルータ認証の設定例です。OSPF ではキー チェーンを使用しません。

interface <インターフェイス> ip ospf message-digest-key <キーID> md5 <パスワード>

router ospf <プロセスID>

network 10.0.0.0 0.255.255.255 area 0 area 0認証メッセージダイジェスト

詳細は、『OSPF の設定』を参照してください。

passive-interface コマンド

ルーティング情報のアドバタイズメントを制御するpassive-interfaceコマンドを使用することで、情報のリーク、つまり不正な情報のIGPへの流入を緩和できます。管理制御の及ばないネットワ

ークへは、情報をいっさいアドバタイズしないでください。

次の例では、この機能の使用方法を示します。

router eigrp <as-number> passive-interface default

no passive-interface <インターフェイス>

ルート フィルタリング

不正なルーティング情報がネットワークに持ち込まれる可能性を減らすために、ルート フィルタリングを使用する必要があります。passive-interface ルータ コンフィギュレーション コマンドとは異なり、ルート フィルタリングがイネーブルになると、ルーティングはインターフェイス上で実行されますが、アドバタイズされる情報や処理される情報は制限されます。

EIGRP および RIP の場合、distribute-list コマンドに out キーワードを指定すると、どの情報をアドバタイズするかが制限され、in キーワードを指定すると、どのアップデートが処理されるのかが制限されます。OSPF では distribute-list コマンドを使用できますが、このコマンドによって、フィルタリングされたルートの伝搬がルータで阻止されることはありません。代わりに、area filter-list コマンドが使用できます。

次の EIGRP の例では、distribute-list コマンドとプレフィクス リストによって発信アドバタイズメントをフィルタリングしています。

ip prefix-list <リスト名>

seq 10 permit <プレフィクス>

router eigrp <as番号>

passive-interface default

no passive-interface <インターフェイス>

distribute-list prefix <リスト名> out <インターフェイス>

次の EIGRP の例では、プレフィクス リストによって着信アップデートをフィルタリングしています。

ip prefix-list <リスト名> seq 10 permit <プレフィックス>

router eigrp <as番号>

passive-interface default

no passive-interface <インターフェイス>

distribute-list prefix <リスト名> in <インターフェイス>

ルーティングアップデートのアドバタイズと処理を制御する方法の詳細は、『EIGRPルートフィルタリング』を参照してください。

次の OSPF の例では、OSPF 固有の area filter-list コマンドとプレフィクス リストを使用しています。

ip prefix-list <リスト名> seq 10 permit <プレフィックス>

router ospf <プロセスID>

area <area-id> filter-list prefix <list-name> in

ルーティング プロセスのリソース消費

ルーティング プロトコル プレフィクスはルータでメモリに保持され、ルータが保持するプレフィクスが増えればリソース消費も上昇します。リソースの枯渇を防ぐために、リソース消費を制限するようにルーティング プロトコルを設定することが重要です。これを OSPF で実現するには、リンクステート データベース過負荷保護機能を使用します。

次の例では、OSPF のリンクステート データベース過負荷保護機能の設定を示しています。

router ospf <プロセスID> max-lsa <最大数>

OSPF のリンクステート データベース過負荷保護の詳細は、『OSPF プロセスでの自己生成 LSA 数の制限』を参照してください。

ファースト ホップ冗長プロトコルの保護

First Hop Redundancy Protocol（FHRP; ファースト ホップ冗長プロトコル）によって、デフォルト ゲートウェイとして機能するデバイスの復元力と冗長性が強化されます。この状況やこれらのプロトコルは、2 台のレイヤ 3 デバイスがネットワーク セグメント、またはサーバやワークステーションを含む VLAN においてデフォルト ゲートウェイとして機能している環境では一般的です。

Gateway Load-Balancing Protocol（GLBP; ゲートウェイ ロードバランシング プロトコル）、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）、および Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、どれも FHRP です。デフォルトでは、これらのプロトコルにより認証なしで通信されます。このような通信では、攻撃者が FHRP に準拠するデバイスになりすましてネットワーク上でデフォルト ゲートウェイの役割を担うことが可能です。このような乗っ取りが行われた場合、攻撃者は中間者攻撃を実行したり、ネットワーク内のすべてのユーザ トラフィックを傍受したりするおそれがあります。

このタイプの攻撃を防ぐために、Cisco IOS XEソフトウェアでサポートされるすべてのFHRPには、MD5またはテキスト文字列を使用した認証機能が組み込まれています。脅威がもたらされるのは認証が行われていない FHRP によるので、これらのプロトコルのインスタンスでは MD5 認証を使用することが推奨されます。次の設定例では、GLBP、HSRP、および VRRP の MD5 認証の使用法を示しています。

インターフェイスFastEthernet 1

glbp認証***ール***説明

glbp 1 authentication md5 key-string <glbp-secret>

glbp 1 ip 10.1.1.1

インターフェイスFastEthernet 2

hsrp認証***説明***

standby 1 authentication md5 key-string <hsrpシークレット>

standby 1 ip 10.2.2.1

インターフェイスFastEthernet 3

vrrp認証***定***説明

vrrp 1 authentication md5 key-string <vrrp-secret>

vrrp 1 ip 10.3.3.1

データ プレーン

データ プレーンは発信元から宛先へのデータの移動を担当しますが、セキュリティという観点では、データ プレーンは 3 つのプレーンの中で最も重要性が低くなっています。このため、ネットワーク デバイスを保護する場合は、データ プレーンよりも管理プレーンとコントロール プレーンを保護することの方が重要です。

ただし、データ プレーン自体にも、トラフィックの保護に役立つ機能や設定オプションが多数あります。以降のセクションでは、ネットワークの保護をより容易にする機能やオプションについて説明しています。

データ プレーン全般の強化

データ プレーン トラフィックの大多数は、ネットワークのルーティング設定に決められたとおりネットワークを通過します。ただし、ネットワークを通過するパケットのパスを変更する IP ネットワーク機能が存在します。IP オプション、とりわけソース ルーティング オプションなどの機能は、今日のネットワークにおけるセキュリティ面の課題です。

また、データ プレーンの強化には、トランジット ACL の使用も関係します。

詳細は、このドキュメントの「通過トラフィックのトランジット ACL によるフィルタリング」の項を参照してください。

IP オプションの選択的廃棄

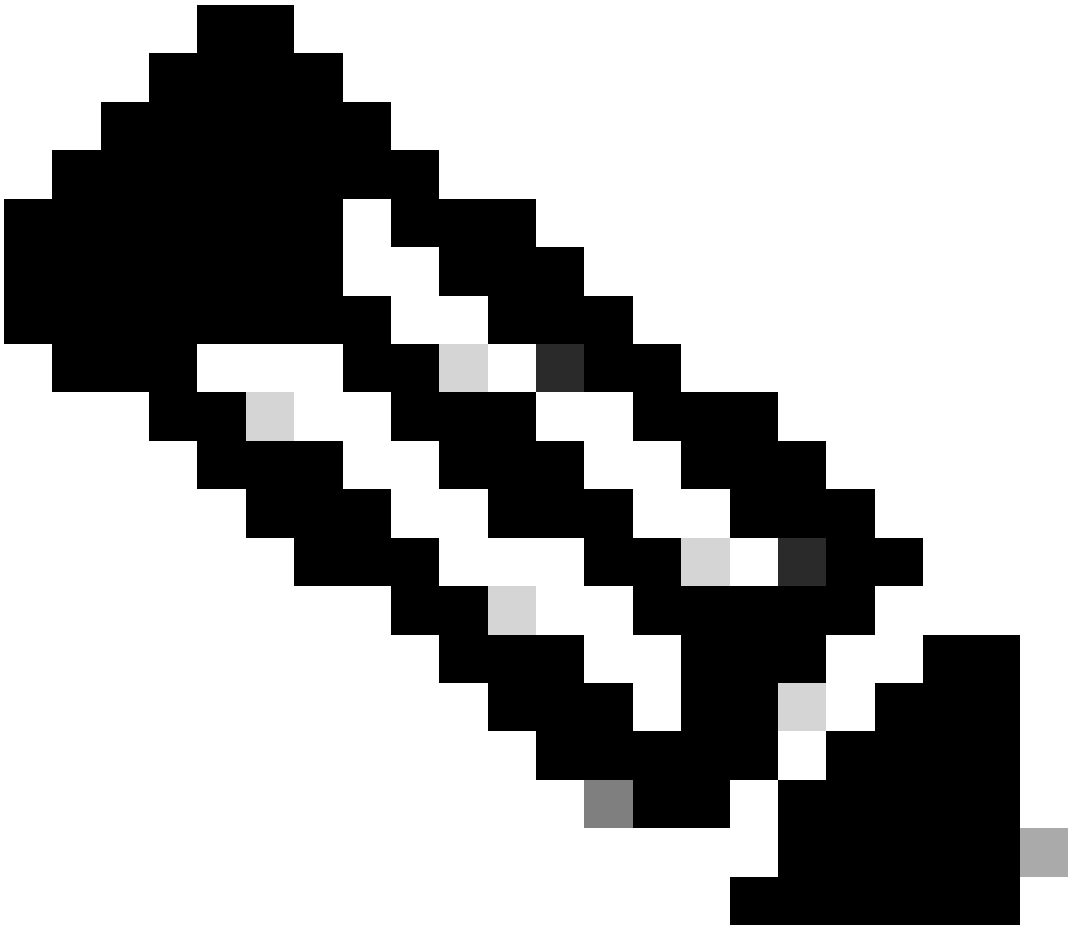
IP オプションに関係するセキュリティの懸念は 2 つあります。IPオプションを含むトラフィックは、Cisco IOS XEデバイスによってプロセススイッチングされる必要があります。これにより、CPU負荷が上昇する可能性があります。また、IP オプションには、ネットワークを通過するトラ

フィックのパスを変更する機能も含まれています。これによりセキュリティ制御が弱体化する可能性があります。

これらの問題、グローバル コンフィギュレーション コマンドipオプションのドロップが原因で | ignore}がCisco IOS XEソフトウェアリリース16.6.4以降に追加されました。最初の形式のip options dropを使用すると、Cisco IOS XEデバイスが受信するIPオプションを含むすべてのIPパケットが廃棄されます。これにより、CPU 負荷の上昇と、IP オプションによって引き起こされる可能性があるセキュリティ制御の弱体化の両方が防止されます。

2番目の形式のip options ignoreを使用すると、受信パケットに含まれるIPオプションが無視されるようにCisco IOS XEデバイスが設定されます。これにより、ローカル デバイスでは IP オプションに関連する脅威が緩和されますが、ダウンストリームのデバイスでは IP オプションの存在による影響を受ける可能性があります。このため、drop 形式でこのコマンドを実行することを強く推奨します。次に、設定例を示します。

IPオプションドロップ



注：一部のプロトコル（RSVPなど）では、IPオプションが正しく使用されます。このよ

うなプロトコルの機能は、このコマンドの影響を受けます。

IP オプションの選択的廃棄をイネーブルにすると、show ip traffic EXEC コマンドを使用して、IP オプションの存在によって廃棄されたパケットの数を把握できます。この情報は、forced drop カウンタに示されます。

この機能についての詳細は、『ACL の IP オプション選択的ドロップ』を参照してください。

IP ソース ルーティングを無効化

IP ソース ルーティングでは、Loose Source Route オプションと Record Route オプションを同時に、または Strict Source Route オプションと Record Route オプションを使用して、パケットが通過するネットワーク パスを IP データグラムのソース側で指定できます。ネットワークのセキュリティ制御に関するトラフィックをルーティングしようとする場合にもこの機能を使用できます。

IP オプションの選択的廃棄機能によって IP オプションを完全にディセーブルにしていない場合は、IP ソース ルーティングをディセーブルにすることが重要です。IPソースルーティングはすべてのCisco IOS XEソフトウェアリリースでデフォルトでイネーブルになっています。これをディセーブルにするには、no ip source-routeグローバルコンフィギュレーションコマンドを使用します。

次の設定例は、このコマンドの使用方法を示しています。

no ip source-route

ICMP リダイレクトのディセーブル化

ICMP リダイレクトは、ネットワーク デバイスに、IP 宛先までのよりよいパスを通知するために使用されます。デフォルトでは、Cisco IOS XEソフトウェアは、受信したインターフェイスを介してルーティングする必要があるパケットを受信すると、リダイレクトを送信します。

状況によっては、攻撃者がCisco IOS XEデバイスに多数のICMPリダイレクトメッセージを送信させ、その結果、CPU負荷が上昇する可能性があります。このため、ICMP リダイレクトの伝送をディセーブルにすることを推奨いたします。ICMP リダイレクトをディセーブルにするには、次の設定例に示すように、インターフェイス コンフィギュレーション コマンド no ip redirects を使用します。

インターフェイスFastEthernet 0

no ip redirects

IP ダイレクト ブロードキャストのディセーブル化または制限

IP ダイレクト ブロードキャストによって、IP ブロードキャスト パケットをリモート IP サブネットに送信できるようになります。パケットがリモート ネットワークに到達すると、フォワーディング IP デバイスによってパケットはレイヤ 2 ブロードキャストとしてサブネット上の全ステー

ションに送信されます。このダイレクトブロードキャスト機能は、smurf攻撃を含むいくつかの攻撃で増幅およびリフレクションの補助手段として利用されています。

現在のバージョンのCisco IOS XEソフトウェアでは、この機能はデフォルトで無効になっています。ただし、ip directed-broadcastインターフェイスコンフィギュレーションコマンドで有効にできます。Cisco IOS XEソフトウェアの12.0より前のリリースでは、この機能はデフォルトで有効になっています。

ネットワークにダイレクトブロードキャスト機能が不可欠な場合は、その使用を制御できます。これを行うには、ip directed-broadcast コマンドのオプションとしてアクセス コントロール リストを使用します。次の設定例では、ダイレクト ブロードキャストを信頼できるネットワーク 192.168.1.0/24 から発信された UDP パケットに制限しています。

access-list 100 permit udp 192.168.1.0 0.0.0.255 any（任意）

インターフェイスFastEthernet 0

IPダイレクトブロードキャスト100

通過トラフィックのトランジット ACL によるフィルタリング

トランジット ACL（tACL）を使用すると、どのトラフィックがネットワークを通過するかを制御できます。これは、ネットワーク自体を宛先とするトラフィックのフィルタリングを行うインフラストラクチャ ACL とは対照的です。特定のデバイス グループへのトラフィックやネットワークを通過しているトラフィックのフィルタリングを行うことが望ましい場合は、tACL によるフィルタリングが便利です。

この種類のフィルタリングは、従来からファイアウォールで実行されています。ただし、ネットワーク内のCisco IOS XEデバイスでこのフィルタリングを実行すると便利な場合があります。たとえば、フィルタリングを実行する必要があっても、ファイアウォールがない場合などです。

トランジット ACL は、静的なアンチスプーフィング保護を実装する場所としても適しています。

詳細は、このドキュメントの「アンチスプーフィング機能」の項を参照してください。

tACL についての詳細は、『トランジット アクセス コントロール リスト：エッジでのフィルタリング』を参照してください。

ICMP パケット フィルタリング

インターネット制御メッセージ プロトコル（ICMP）は、IP 用のコントロール プロトコルとしての設計になっています。そのため、伝送されるメッセージは、一般にTCPおよびIPプロトコルに広範囲にわたる影響を及ぼす可能性があります。ネットワーク トラブルシューティング ツールの ping や traceroute、およびパス MTU ディスカバリでは ICMP が使用されますが、ネットワークが正常に動作している場合、外部 ICMP 接続が必要になることはほとんどありません。

Cisco IOS XEソフトウェアには、名前またはタイプとコードによってICMPメッセージを明確にフィルタリングする機能があります。次の例の ACL は、信頼できるネットワークからの ICMP を

許可し、それ以外の発信元からのすべての ICMP パケットをブロックしています。

ipアクセスリスト拡張ACLトランジットイン

---信頼できるネットワークからの ICMP パケットのみを許可します。

permit icmp host <信頼できるネットワーク> any

---任意のネットワーク デバイスに対するその他の IP トラフィックをすべて拒否します。

deny icmp any any

IP フラグメントのフィルタリング

このドキュメントの「インフラストラクチャ ACL によるネットワーク アクセス制限」の項で説明したように、フラグメント化された IP パケットのフィルタリングは、セキュリティ デバイスにとっての課題です。

フラグメント処理はわかりにくいため、IP フラグメントが誤って ACL によって許可されることがあります。また、侵入検知システムによる検出を逃れようとして、フラグメンテーションが使用されることもよくあります。このような理由から、IPフラグメントは攻撃で使用されることが多く、設定されたtACLの先頭で明示的にフィルタリングできます。

ACLには、IPフラグメントの包括的なフィルタリングが含まれます。次の例の機能は、これまでの例の機能と組み合わせて使用する必要があります。

ipアクセスリスト拡張ACLトランジットイン

– プロトコル固有のACEを使用するIPフラグメントを拒否して、

---IP フラグメントを拒否します。

deny tcp any any fragments (任意のフラグメントを拒否)

deny udp any any fragments (すべてのフラグメントをUDPに拒否)

deny icmp any any fragments (icmpの任意のフラグメント)

deny ip any any fragments (どのフラグメントでも拒否)

フラグメント化されたIPパケットのACLによる処理の詳細は、『フラグメントのアクセスリスト処理』を参照してください。

IP オプションのフィルタリングの ACL サポート

Cisco IOS XEソフトウェアリリース16.6.4以降、Cisco IOS XEソフトウェアは、ACLを使用して、パケットに含まれるIPオプションに基づいてIPパケットをフィルタリングする機能をサポートしています。パケット内にIPオプションが存在する場合は、ネットワーク内のセキュリティ制御を弱体化させようとしているか、パケットの伝送特性を変更しようとしている可能性があります。このような理由から、IPオプション付きのパケットは、ネットワークのエッジでフィルタリン

グできます。

IP オプションを含む IP パケットに対して完全なフィルタリングを行うには、次の例をこれまでの例の内容と組み合わせて使用する必要があります。

ipアクセスリスト拡張ACLトランジットイン

— IPオプションを含むIPパケットを拒否

deny ip any anyオプションany-options

アンチスプーフィング保護

攻撃の多くは、効果を高めるためや、攻撃の実際の発信元の隠蔽や正確なトレースバックの妨害のために、発信元 IP アドレスのスプーフィングを利用しています。Cisco IOS XEソフトウェアには、送信元IPアドレスのスプーフィングに基づく攻撃を防止するために、ユニキャストRPFとIPソースガード(IPSG)が用意されています。さらに、多くの場合、スプーフィングを手動で阻止する手段として ACL とヌル ルーティングが展開されます。

IP ソース ガードは、スイッチ ポート、MAC アドレス、および発信元アドレスの検証を行うことによって、直接の管理制御下にあるネットワークに対するスプーフィングを最小に抑えることができます。ユニキャスト RPF では、発信元ネットワークの検証が行われ、直接の管理制御下にないネットワークからのスプーフィング攻撃を抑制できます。ポート セキュリティを使用すると、アクセス レイヤで MAC アドレスの検証が行われます。Dynamic Address Resolution Protocol（ARP）Inspection（DAI）により、ローカル セグメントの ARP ポイズニングを利用する攻撃が抑制されます。

ユニキャスト RPF

ユニキャスト RPF では、転送されたパケットを受信したインターフェイスを介して、そのパケットの発信元アドレスに到達できるかどうかをデバイスで確認できます。スプーフィング対策をユニキャスト RPF だけに依存しないでください。送信元IPアドレスへの適切なリターンルートが存在する場合、スプーフィングされたパケットは、ユニキャストRPFが有効なインターフェイスを介してネットワークに侵入する可能性があります。ユニキャスト RPF を使用するには、各デバイスで Cisco エクスプレス フォワーディングがイネーブルになっている必要があります。ユニキャスト RPF はインターフェイスごとに設定されます。

ユニキャスト RPF には loose と strict という 2 つの動作モードがあり、どちらかを設定します。非対称ルーティングが存在する場合は、loose モードを推奨いたします。strict モードではこのような場合、パケットが廃棄されるからです。ip verify インターフェイス コンフィギュレーション コマンドの設定で、キーワード any を指定すると loose モード、キーワード rx を指定すると strict モードになります。

次の例は、この機能の設定を示しています。

ip cef

interface <インターフェイス>

ip verify unicast source reachable-via <モード>

ユニキャスト RPF の設定と使用法についての詳細は、『ユニキャスト リバース パス転送について』を参照してください。

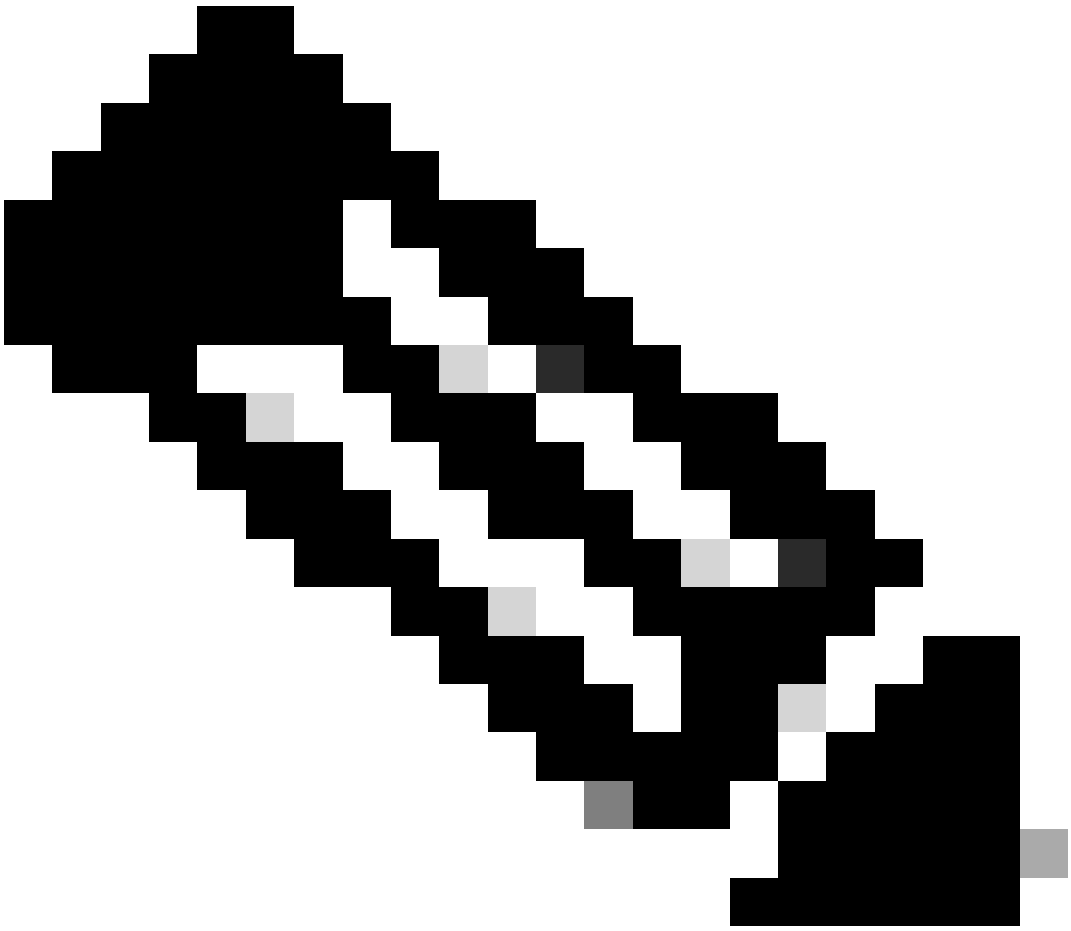
IP ソース ガード

レイヤ 2 インターフェイスを制御できる場合、IP ソース ガードはスプーフィングを防止する有効な手段です。IP ソース ガードは、DHCP スヌーピングからの情報を使用して、レイヤ 2 インターフェイス上にポート アクセス コントロール リスト（PACL）を動的に設定し、IP ソース バインディング テーブルに関連付けられていない IP アドレスからのトラフィックを拒否します。

IP ソース ガードは、DHCP スヌーピングがイネーブルの VLAN に属するレイヤ 2 インターフェイスに適用できます。DHCP スヌーピングは次のコマンドによってイネーブルになります。

ip dhcpスヌーピング

ip dhcp snooping vlan <vlan範囲>



注:IP Source Guardをサポートするには、シャーシ/ルータにレイヤ2スイッチングモジュールが必要です。

ポート セキュリティをイネーブルにするには、ip verify source port security インターフェイス コンフィギュレーション コマンドを使用します。これには、グローバル コンフィギュレーション コマンド ip dhcp snooping information option を実行する必要があります。さらに、DHCP サーバが DHCP オプション 82 をサポートしている必要があります。

この機能についての詳細は、『IPソースガード』を参照してください。

ポート セキュリティ

ポート セキュリティを使用すると、アクセス インターフェイスでの MAC アドレスのスプーフィングが抑制されます。ポート セキュリティでは、動的に学習された (スティッキ) MAC アドレスを使用することで、初期設定が容易になります。ポート セキュリティによって MAC 違反が特定されると、4 つの違反モードのいずれかが適用されます。これには protect、restrict、shutdown、および shutdown VLAN のモードがあります。ポートが標準プロトコルを使用して1台のワークステーションだけにアクセスを提供する場合は、最大数の1で十分です。最大数が 1 に設定された場合、バーチャル MAC アドレスを使用する HSRP などのプロトコルは機能しません。

interface <インターフェイス> switchport

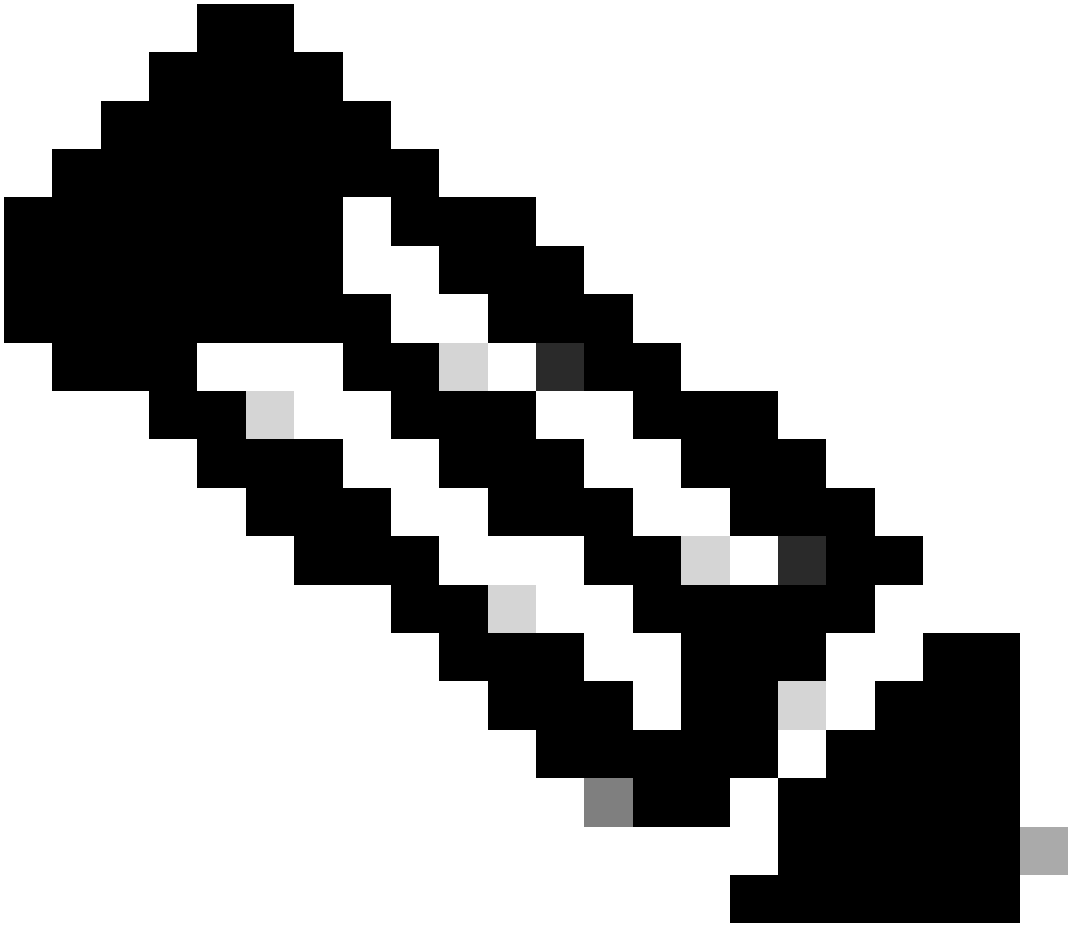
switchport mode access

switchport port-securityコマンド

switchport port-security mac-address sticky

switchport port-security maximum <番号>

switchport port-security violation <違反モード>



注：ポートセキュリティをサポートするには、シャーシ/ルータにレイヤ2スイッチングモジュールが必要です。

ポートセキュリティ設定についての詳細は、『ポートセキュリティの設定』を参照してください。

アンチスプーフィング ACL

手動で設定された ACL は、既知で未使用のアドレス レンジや信頼できないアドレス レンジを使用する攻撃に対して、静的なアンチスプーフィング機能を提供します。通常、このようなアンチスプーフィング ACL は、より大規模な ACL のコンポーネントとしてネットワーク バウンダリで入トラフィックに適用されます。アンチスプーフィング ACL は頻繁に変更されることがあるので、定期的に監視する必要があります。送信 ACL を適用してトラフィックを有効なローカル アドレスに制限すると、ローカル ネットワークから発信するトラフィックでのスプーフィングを最小に抑えることができます。

次の例は、ACL を使用して IP スプーフィングを制限する方法を示しています。この ACL は、対

象のインターフェイスの着信側に適用されます。この ACL を構成する ACE は、すべてを網羅しているわけではありません。このような種類の ACL を設定する場合、確実な最新の参照を含めるようにしてください。

ipアクセスリスト拡張ACL-ANTISPOOF-IN

deny ip 10.0.0.0 0.255.255.255 any

deny ip 192.168.0.0 0.0.255.255 any

interface <インターフェイス>

ip access-group ACL-ANTISPOOF-INを

アクセスコントロールリストの設定方法の詳細については、『IPv4 ACLの設定』を参照してください。

データ プレーン トラフィックの CPU への影響の制限

ルータとスイッチの主目的は、パケットやフレームをデバイス経由で最終的な宛先まで転送することです。これらのパケットは、ネットワーク上に展開されたデバイスを通過するので、デバイスの CPU 動作に影響を及ぼす可能性があります。データプレーンは、ネットワークデバイスを通過するトラフィックで構成され、管理プレーンとコントロールプレーンの動作を保証するために保護できます。通過トラフィックによってデバイスでスイッチトラフィックが処理される可能性がある場合、デバイスのコントロールプレーンが影響を受け、運用が中断される可能性があります。

CPU に影響する機能とトラフィックの種類

特別な CPU 処理を必要とするデータ プレーン トラフィックを以下に示します。これらのトラフィックは CPU でプロセス スイッチングされます。ただし、これはすべてを網羅したリストではありません。

1. ACL ロギング：ACL ロギング トラフィックは、log キーワードが使用された場合の ACE の一致（許可または拒否）によって生成されるパケットで構成されます。
2. ユニキャストRPF：ユニキャストRPFがACLとともに使用される場合、特定のパケットのプロセススイッチングが行われる可能性があります。
3. IP オプション：オプションが指定された任意の IP パケットは、CPU で処理する必要があります。
4. フラグメンテーション：フラグメンテーションを必要とする任意の IP パケットは、CPU に渡して処理する必要があります。
5. 存続可能時間（TTL）の期限切れ：TTL 値が 1 以下のパケットでは、インターネット制御メッセージ プロトコルの Time Exceeded（ICMP タイプ 11、コード 0）メッセージが送信される必要があります。これにより CPU 処理が発生します。
6. ICMP 到達不能：ルーティング、MTU、またはフィルタリングによって ICMP 到達不能メッセージを発生させるパケットは、CPU で処理されます。
7. ARP 要求を必要とするトラフィック：ARP エントリが存在しない宛先は、CPU での処理が

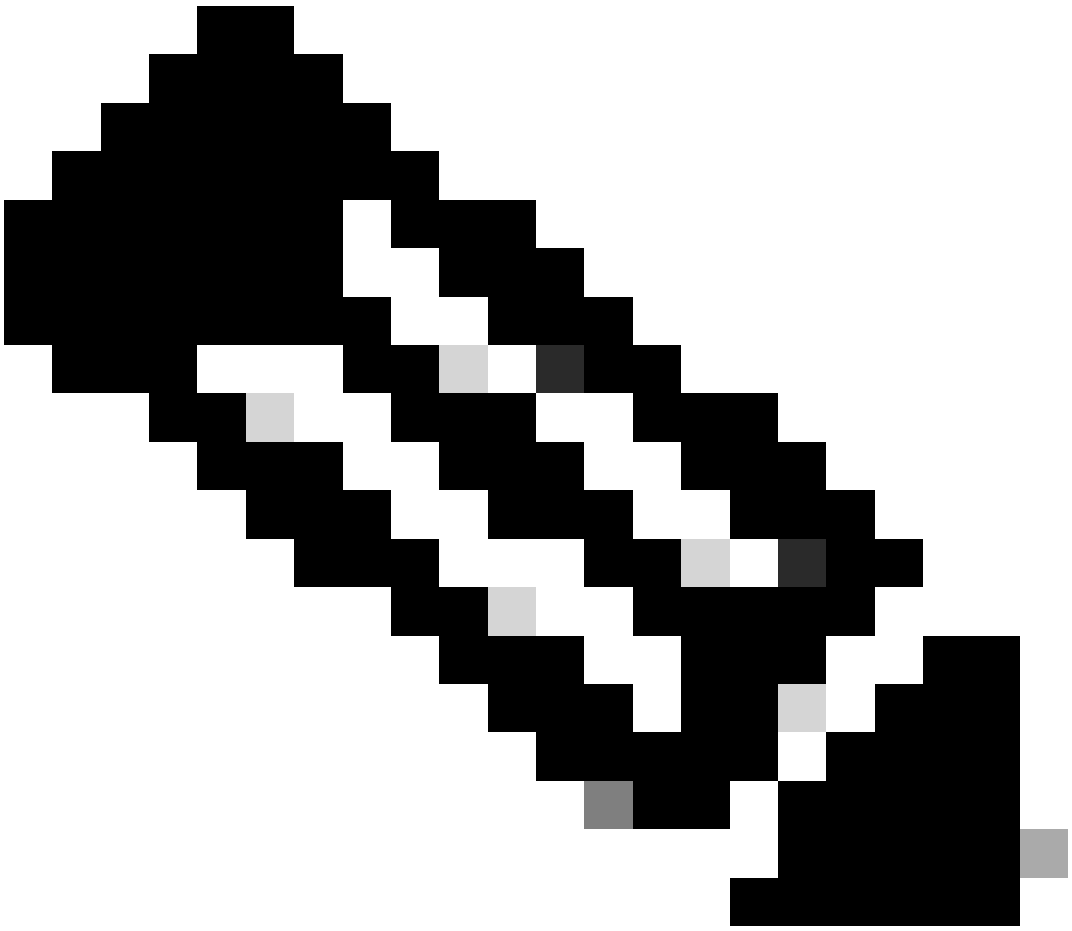
必要です。

8. 非 IP トラフィック：すべての非 IP トラフィックは CPU で処理されます。

   データ プレーンの強化の詳細については、このドキュメントの「データ プレーン全般の強化」の項を参照してください。

TTL 値に基づくフィルタ

ACLのTTL値フィルタリングサポート機能は、Cisco IOS XEソフトウェアリリース16.6.4で導入されました。この機能を拡張IPアクセスリストで使用すると、TTL値に基づいてパケットをフィルタリングできます。この機能を使用すると、TTL 値が 0 または 1 の通過トラフィックを受信するデバイスを保護できます。また、TTL値に基づくパケットのフィルタリングを使用して、TTL値がネットワークの直径を下回らないようにすることもできます。これにより、ダウンストリームインフラストラクチャデバイスのコントロールプレーンがTTL超過攻撃から保護されます。



注：アプリケーションやtracerouteなどのツールでは、テストや診断のためにTTL期限切れパケットが使用されます。IGMP など一部のプロトコルでは、TTL 値が 1 のパケットが正規の目的で使用されます。

次の ACL の例では、TTL 値が 6 未満の IP パケットをフィルタリングするポリシーが作成されます。

— TTL値を持つIPパケットをフィルタリングするACLポリシーを作成します。

— 6未満

ipアクセスリスト拡張ACLトランジットイン

deny ip any any ttl lt 6

permit ip any any（任意のIPを許可）

– インターフェイスに入力方向でアクセスリストを適用します。

interface GigabitEthernet0/0

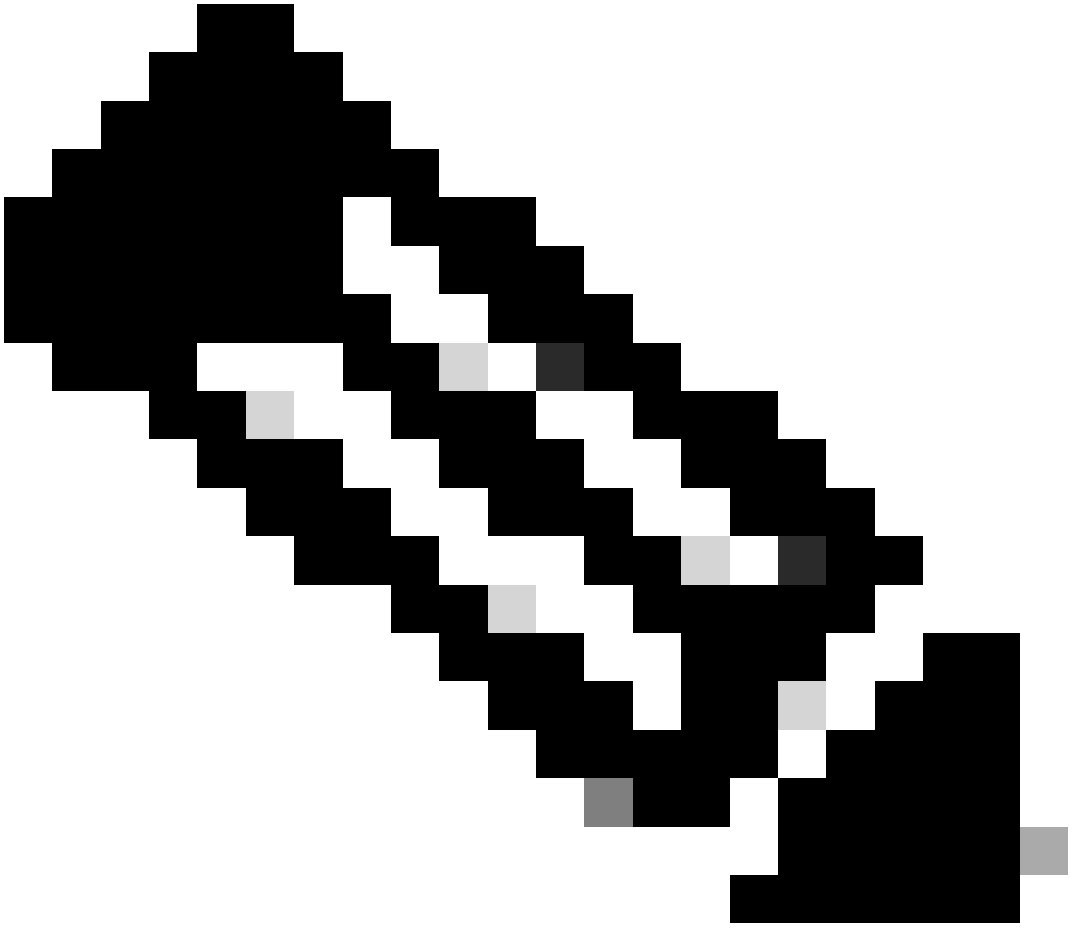
ip access-group ACL-TRANSIT-IN

TTL 値に基づくパケット フィルタリングについての詳細は、『TTL 超過攻撃の識別と緩和』を参照してください。

この機能についての詳細は、『ACL の TTL 値フィルタリング サポート』を参照してください。

IP オプションの有無によるフィルタ

Cisco IOS XEソフトウェアリリース16.6.4以降では、名前付き拡張IPアクセスリストでACLのIPオプションフィルタリングサポート機能を使用して、IPオプションが存在するIPパケットをフィルタリングできます。IPオプションの存在に基づくIPパケットのフィルタリングも、インフラストラクチャデバイスのコントロールプレーンがこれらのパケットをCPUレベルで処理しなければならないことを防ぐために使用できます。



注:ACLのIPオプションフィルタリングサポート機能は、名前付き拡張ACLでのみ使用できます。

また、RSVP、マルチプロトコルラベルスイッチングトラフィックエンジニアリング、IGMPバージョン2と3、およびIPオプションパケットを使用するその他のプロトコルは、これらのプロトコルのパケットが廃棄されると、正常に機能できないことに注意してください。これらのプロトコルがネットワークで使用されている場合は、ACLのIPオプションフィルタリングサポート機能も使用できます。ただし、ACLのIPオプション選択的廃棄機能によってこれらのトラフィックが廃棄される可能性があり、これらのプロトコルは適切に機能しません。これらのパケットの廃棄に ACL の IP オプション選択的廃棄が推奨されるのは、IP オプションを必要とするプロトコルが使用されていない場合です。

次の ACL の例では、IP オプションを含む IP パケットをフィルタリングするポリシーが作成されます。

ipアクセスリスト拡張ACLトランジットイン

deny ip any anyオプションany-options

permit ip any any（任意のIPを許可）

interface GigabitEthernet0/0

ip access-group ACL-TRANSIT-IN

次の ACL の例では、特定の 5 つの IP オプションを含む IP パケットをフィルタリングするポリシーを示しています。次のオプションを含むパケットが拒否されます。

1. 0 オプション リストの終端（eool）
2. 7 ルートの記録（record-route）
3. 68 タイム スタンプ（timestamp）
4. 131 ルース ソース ルート（lsr）
5. 137 ストリクト ソース ルート（ssr）

ipアクセスリスト拡張ACLトランジットイン

deny ip any anyオプションeool

deny ip any anyオプションrecord-route

deny ip any anyオプションタイムスタンプ

deny ip any anyオプションlsr

deny ip any anyオプションssr

permit ip any any（任意のIPを許可）

interface GigabitEthernet0/0

ip access-group ACL-TRANSIT-IN

ACL の IP オプション選択的廃棄についての詳細は、このドキュメントの「データ プレーン全般の強化」の項を参照してください。

Cisco IOS XEソフトウェアのもう1つの機能で、IPオプションを使用してパケットをフィルタリングするために使用できる機能がCoPPです。Cisco IOS XEソフトウェアリリース16.6.4以降では、CoPPを使用してコントロールプレーンパケットのトラフィックフローをフィルタリングできます。Cisco IOS XEソフトウェアリリース16.6.4で導入された、CoPPおよびACLのIPオプションフィルタリングサポートをサポートするデバイスは、アクセスリストポリシーを使用して、IPオプションを含むパケットをフィルタリングできます。

次の CoPP ポリシーでは、デバイスで受信される通過パケットに IP オプションが付いている場合、そのパケットが廃棄されます。

ipアクセスリスト拡張ACL-IP-OPTIONS-ANY

permit ip any anyオプションany-options

クラスマップACL-IP – オプション – クラス

match access-group name ACL-IP-OPTIONS-ANY（オプションの一致）

ポリシーマップCOPPポリシー

クラスACL-IP – オプション – クラス

police 80000 conform transmit exceed drop（ポリシング送信超過ドロップ）

control-plane

service-policy input COPP-POLICY !

次の CoPP ポリシーでは、デバイスで受信される通過パケットに次の IP オプションが付いている場合、そのパケットが廃棄されます。

1. 0 オプション リストの終端（eool）
2. 7 ルートの記録（record-route）
3. 68 タイム スタンプ（timestamp）
4. 131 ルース ソース ルート（lsr）
5. 137 ストリクト ソース ルート（ssr）

ipアクセスリスト拡張ACL IPオプション

permit ip any anyオプションeool

permit ip any anyオプションrecord-route

permit ip any anyオプションタイムスタンプ

permit ip any anyオプションlsr

permit ip any anyオプションssr

クラスマップACL-IP – オプション – クラス

match access-group name ACL-IP – オプション

ポリシーマップCOPPポリシー

クラスACL-IP – オプション – クラス

police 80000 conform transmit exceed drop（ポリシング送信超過ドロップ）

control-plane

service-policy input COPP-POLICY（サービスポリシー入力COPPポリシー）

前述のCoPPポリシーでは、アクセスコントロールリストエントリ(ACE)のpermitアクションに一致するパケットがある場合、このようなパケットはポリシーマップのdrop機能によって廃棄されますが、denyアクション（非表示）に一致するパケットは、ポリシーマップのdrop機能の影響を受けません。

CoPP 機能についての詳細は、『コントロール プレーン ポリシングの展開』を参照してください。

コントロール プレーン保護

Cisco IOS XEソフトウェアリリース16.6.4以降では、コントロールプレーン保護(CPPr)を使用して、Cisco IOS XEデバイスのCPUによるコントロールプレーントラフィックを制限またはポリシングできます。CPPrはCoPPと同様に、CoPPよりも細かい制御を使用するトラフィックを制限またはポリシングできます。CPPr によって集約コントロール プレーンは、サブインターフェイスと呼ばれる 3 つの個別のコントロール プレーン カテゴリに分割されます。Host、Transit、および CEF-Exception というサブインターフェイスが存在します。

次の CPPr ポリシーでは、デバイスで受信される通過パケットの TTL 値が 6 未満の場合、またはデバイスで受信される通過パケットや非通過パケットの TTL 値が 0 か 1 の場合、そのパケットは廃棄されます。さらに、デバイスで受信されるパケットに指定の IP オプションが付いている場合、そのパケットもドロップされます。

ipアクセスリスト拡張ACL-IP-TTL-0/1

permit ip any any ttl eq 0 1

クラスマップACL-IP-TTL-0/1-CLASS

match access-group名前ACL-IP-TTL-0/1

ipアクセスリスト拡張ACL-IP-TTL-LOW

permit ip any any ttl lt 6

クラスマップACL-IP-TTL-LOW-CLASS

match access-group name ACL-IP-TTL-LOW（オプション）

ipアクセスリスト拡張ACL IPオプション

permit ip any anyオプションeool

permit ip any anyオプションrecord-route

permit ip any anyオプションタイムスタンプ

permit ip any anyオプションlsr

permit ip any anyオプションssr

クラスマップACL-IP – オプション – クラス

match access-group name ACL-IP – オプション

ポリシーマップCPPR-CEF-EXCEPTION-POLICY

クラスACL-IP-TTL-0/1-CLASS

police 80000 conform-action drop（適合アクション廃棄）

クラスACL-IP – オプション – クラス

police 8000 conform-action drop（準拠アクション廃棄）

ポリシーマップCPPR-TRANSIT-POLICY

クラスACL-IP-TTL-LOW-CLASS

police 8000 conform-action drop（準拠アクション廃棄）

コントロールプレーン中継

service-policy入力CPPR-TRANSIT-POLICY

前述の CPPr ポリシーでは、アクセス コントロール リスト エントリの permit アクションに一致するパケットがある場合、このようなパケットはポリシーマップの drop 機能によって廃棄されますが、deny アクション（非表示）に一致するパケットは、ポリシーマップの drop 機能の影響を受けません。

CPPr機能についての詳細は、『コントロールプレーンポリシング』を参照してください。

トラフィックの識別とトレースバック

場合によっては、ネットワークトラフィックを迅速に特定してトレースバックする必要があります。特に、インシデントへの対応やネットワークパフォーマンスの低下の際に重要になります。Cisco IOS XEソフトウェアでこれを実現する主な方法は、NetFlowと分類ACLの2つです。NetFlow を使用すると、ネットワーク上のすべてのトラフィックを把握できます。さらに、NetFlowは、長期的なトレンド分析と自動分析を提供するコレクタとともに実装できます。分類 ACL は、ACL のコンポーネントであり、トラフィックを識別するための事前計画と分析中の手動介入が必要です。以下のセクションでは、これらの機能の簡単な概要を示します。

NetFlow

NetFlow は、ネットワーク フローをトラッキングすることで、異常なネットワーク アクティビティやセキュリティに関係するネットワーク アクティビティを特定します。NetFlow のデータは、CLI から表示と分析ができます。また、市販またはフリーウェアの NetFlow コレクタにデータをエクスポートして、集計や分析を行うこともできます。NetFlow コレクタは、長期的なトレンディングから、ネットワーク動作や使用状況を分析できます。NetFlow は、IP パケット内の特定のアトリビュートを分析し、フローを作成することによって機能します。最もよく使用されている NetFlow のバージョンは 5 ですが、バージョン 9 の方が拡張性に富んでいます。NetFlow のフローは、高ボリュームの環境でサンプリングされたトラフィック データを使用して作成できます。

NetFlowをイネーブルにするには、CEF、つまり分散CEFが前提条件です。NetFlow はルータやスイッチ上で設定できます。

次の例では、この機能の基本設定を示しています。Cisco IOS XEソフトウェアのこれまでのリリースでは、インターフェイスでNetFlowを有効にするコマンドは、ip route-cache flowです(ip flow {ingress | egress} ではありません ）。

ip flow-export destination <ipアドレス> <udpポート>

ip flow-export version <バージョン>

interface <インターフェイス>

ip flow <入力|出力>

CLI からの NetFlow の出力例を次に示します。SrcIf アトリビュートはトレースバックに使用できます。

router#show ip cache flow IP packet size distribution(26662860パケット合計):

1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480

.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IPフロースイッチングキャッシュ、4456704バイト

55アクティブ、65481非アクティブ、1014683追加

41000680 agerポーリング、0フロー割り当てエラー

アクティブなフローが2分でタイムアウト

非アクティブなフローが60秒後にタイムアウト

IPサブフローキャッシュ、336520バイト

110アクティブ、16274非アクティブ、2029366追加、1014683フローへの追加

割り当てエラーが0個、強制解放が0個、15個のチャンクが追加され、統計情報の最後のクリアは実行されない

プロトコル合計フローパケットバイトアクティブなパケット（秒）アイドル状態（秒）

--------フロー/Sec /Flow /Pkt /Sec /Flow /Flow

TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8

TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1

TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1

TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5

TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4

TCP-X 351 0.0 2 40 0.0 0.0 60.8

TCP-BGP 114 0.0 1 40 0.0 0.0 62.4

TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4

TCP-other 556070 0.6 8 318 6.0 8.2 38.3

UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1

UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6

UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2

UDP-Frag 1 0.0 1405 0.0 0.0 86.8

UDPその他86247 0.1 226 29 24.0 31.4 54.3

ICMP 19989 0.0 37 33 0.9 26.0 53.9

IP-other 193 0.0 1 22 0.0 3.0 78.2

合計：1014637 1.2 26 99 32.8 13.8 43.9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts

Gi0/1 192.168.128.21ローカル192.168.128.20 11 CB2B 07AF 3

Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9

Gi0/1 192.168.150.60ローカル192.168.206.20 01 0000 0303 11

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1

NetFlowの機能の詳細は、『Flexible NetFlow』を参照してください。

分類 ACL

分類 ACL を使用すると、インターフェイスを通過するトラフィックを把握できます。分類 ACL によって、ネットワークのセキュリティ ポリシーが変更されることはありません。通常、分類 ACL は、個別のプロトコル、発信元アドレス、または宛先を分類するように作成されます。たとえば、すべてのトラフィックを許可する ACE は、プロトコル単位、またはポート単位に分類できます。各トラフィック カテゴリにヒット カウンタが付いているので、トラフィックを特定の ACE へと詳細に分類することで、ネットワーク トラフィックを把握しやすくなります。また、ACLの最後にある暗黙的なdenyを詳細なACEに分割して、拒否されたトラフィックのタイプを特定することもできます。

管理者は、show access-list EXECコマンドおよびclear ip access-list counters EXECコマンドで分類ACLを使用することにより、インシデント対応を迅速化できます。

次の例では、デフォルトの deny の前に SMB トラフィックを識別する分類 ACL の設定を示しています。

ipアクセスリスト拡張ACL-SMB-CLASSIFY

aclの既存の内容を再マーキングする

smb固有のTCPトラフィックのremark分類

deny tcp any any eq 139（tcpの任意のeqを拒否）

deny tcp any any eq 445

deny ip any any

分類ACLを使用するトラフィックを識別するには、show access-list acl-name

EXECコマンドを使用します。ACLカウンタをクリアするには、clear ip access-list counters aclname EXECコマンドを使用します。

router#show access-list ACL-SMB-CLASSIFY拡張IPアクセスリストACL-SMB-CLASSIFY

10 deny tcp any any eq 139（10件の一致）

20 deny tcp any any eq 445（9件の一致）

30 deny ip any any（184一致）

ACL のロギング機能をイネーブルにする方法についての詳細は、『アクセス コントロール リストのロギングについて』を参照してください。

PACL によるアクセス コントロール

PACL を適用できるのは、スイッチのレイヤ 2 物理インターフェイスの着信側のみです。PACL では VLAN マップと同様に、ルーティングされていないトラフィックやレイヤ 2 トラフィックに対してアクセス コントロールが適用されます。PACL を作成するための構文はルータ ACL と同じであり、PACL は VLAN マップおよびルータ ACL より優先されます。レイヤ 2 インターフェイスに適用される ACL は、PACL と呼ばれます。

設定では、IPv4、IPv6、または MAC の ACL の作成と、レイヤ 2 インターフェイスへの適用を行います。

次の例では、名前付き拡張アクセス リストを使用し、この機能の設定を示しています。

ip access-list extended <acl-name> permit <protocol> <source-address> <source-port> <destination-address> <destination-port> !

interface <type> <slot/port> switchport mode access switchport access vlan <vlan_number> ip access-group <acl-name> in !

PACLの設定についての詳細は、『ポートACLによるネットワークセキュリティの設定』のポートACLに関するセクションを参照してください。

隔離 VLAN

セカンダリ VLAN を隔離 VLAN として設定することで、セカンダリ VLAN 内のデバイス間の通信を完全に禁止できます。プライマリVLANごとに隔離VLANは1つのみ設定でき、隔離VLAN内のポートと通信できるのは混合ポートだけです。隔離VLANは、ゲストをサポートするネットワークなどの信頼できないネットワークで使用できます。

次の設定例では、VLAN 11 を隔離 VLAN として設定し、プライマリ VLAN である VLAN 20 に関連付けています。また、この例では、インターフェイスFastEthernet 1/1をVLAN 11の隔離ポートとして設定しています。

vlan 11プライベートvlan隔離

vlan 20プライベートvlanプライマリプライベートvlanアソシエーション11

インターフェイスFastEthernet 1/1の説明***隔離VLANのポート*** switchport mode private-vlan host switchport private-vlan host-association 20 11

コミュニティ VLAN

セカンダリ VLAN がコミュニティ VLAN として設定されている場合、VLAN のメンバ間の通信は許可され、プライマリ VLAN の任意の混合モード ポートを使用できます。ただし、2 つのコミュニティ VLAN 間の通信や、コミュニティ VLAN から隔離 VLAN への通信は許可されません。サーバを相互に接続する必要があるが、VLAN 内のその他のデバイスと接続する必要はない場合、サーバをグループ化するには、コミュニティ VLAN を使用する必要があります。これは、一般アクセスが可能なネットワークや、信頼できないクライアントにサーバがコンテンツを提供する場合に一般的なシナリオです。

次の例では、1 つのコミュニティ VLAN を設定し、スイッチ ポート FastEthernet 1/2 をその

VLAN のメンバとして設定しています。コミュニティ VLAN である VLAN 12 は、プライマリ VLAN である VLAN 20 に対してセカンダリ VLAN です。

vlan 12プライベートvlanコミュニティ

vlan 20プライベートvlanプライマリプライベートvlanアソシエーション12

インターフェイスFastEthernet 1/2の説明***コミュニティVLANのポート*** switchport mode private-vlan host switchport private-vlan host-association 20 12

結論

このドキュメントでは、Cisco IOS XEシステムデバイスを保護するために使用できる方法の概要について説明します。デバイスを保護することで、管理対象のネットワークの全体的なセキュリティが高まります。この概要では、管理プレーン、コントロール プレーン、およびデータ プレーンの保護について説明し、設定に関する推奨事項を示しています。関連のある各機能の設定については、可能な限り、十分詳しく説明しています。ただし、より詳しい評価に必要な情報を提供するためには、すべての場合で包括的な参照先を示しています。

確認

このマニュアルのある機能についてはシスコの情報の開発チームで記述されます。

付録：Cisco IOS XEデバイス強化のチェックリスト

このチェックリストでは、このガイドの強化手順の集合です。

管理者は、Cisco IOS XEデバイスで使用および考慮したすべての強化機能を思い出させるために、この機能を使用できます。これは、該当しない機能が実装されていないとしても可能です。管理者は、オプションには潜在的リスクの各オプションを評価することを推奨します。

管理プレーン

1. パスワード
   イネーブルパスワードとローカルユーザパスワードのMD5ハッシュ（シークレットオプション）を有効にするパスワード再試行ロックアウトを設定するパスワード回復を無効にする（リスクを考慮する）
2. 使用していないサービスを無効にする
3. 管理セッションのTCPキープアライブを設定します
4. メモリおよびCPUしきい値通知を設定します
5. 設定
   メモリおよびCPUしきい値通知コンソールアクセス用のメモリ予約メモリリーク検出バッファオーバーフロー検出クラッシュ情報の収集の強化
6. 管理アクセスを制限するのにiACLsを使用します
7. フィルタリング（リスクを考慮します）
   ICMPパケットIPフラグメントIPオプションTTL値（パケット単位）

8. コントロール プレーン保護
   ポートフィルタリングの設定キューしきい値の設定
9. 管理アクセス
   管理インターフェイスを制限するために管理プレーン保護を使用するexecタイムアウトを設定するCLIアクセスに暗号化トランスポートプロトコル（SSHなど）を使用するvty回線とtty回線のトランスポートを制御する（アクセスクラスオプション）バナーを使用する警告を表示する
10. [AAA]
    認証とフォールバックにAAAを使用コマンド許可にAAA(TACACS+)を使用アカウンティングにAAAを使用する冗長AAAサーバを使用する
11. SNMP
    SNMPv2コミュニティの設定とACLの適用SNMPv3の設定
12. Logging
    中央集中型ロギングの設定関連するすべてのコンポーネントのロギングレベルの設定ロギングソースインターフェイスの設定ロギングタイムスタンプの精度の設定
13. 構成管理
    置き換えとロールバック排他コンフィギュレーション変更アクセスソフトウェア復元カコンフィギュレーションコンフィギュレーション変更通知。

コントロール プレーン

1. 無効にリスクを考慮します）
   ICMPリダイレクトICMP到達不能プロキシARP
2. NTPを使用する場合はNTP認証を設定する
3. 設定するコントロール プレーン ポリシング/保護（ポートのフィルタリング、キューしきい値）
4. ルーティング プロトコルを保護する
   BGP（TTL、MD5、最大プレフィクス、プレフィックスリスト、システムパス
   ACL）IGP（MD5、パッシブインターフェイス、ルートフィルタリング、リソース消費）
5. ハードウェア レート リミッタを設定します
6. セキュア ファーストホップ冗長プロトコル（GLBP、HSRP、VRRP）

データ プレーン

1. IP オプションの選択的ドロップを設定する
2. 無効にリスクを考慮します）
   IPソースルーティングIPダイレクトブロードキャストICMPリダイレクト
3. IP ダイレクト ブロードキャストを制限する
4. tACLsを設定します（リスクを考慮します）
   フィルタIPフラグメントIPオプションフィルタTTL値
5. configureアンチスプーフィング保護を必要とする
   ACL IPソースガードダイナミックARPインスペクションユニキャストARPポートセキュリティ
6. コントロール プレーン保護（コントロール プレーンcef例外）
7. トラフィックを識別するためのNetFlowおよび分類ACLを設定します

8. configure必要なアクセス コントロールACL（ VLANマップ、PACL、MAC ）
9. プライベート VLAN を設定する

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。