CHAPTER 1

概要

Cisco NX-OS がサポートするセキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

ここでは、次の内容を説明します。

AAA

Authenticaiton, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）は、3 つの独立したセキュリティ機能をまとめて一貫性のあるモジュラ形式で設定するためのアーキテクチャ フレームワークです。

- 認証 — ログイン / パスワード ダイアログ、チャレンジ / レスポンス、メッセージング サポート、および選択したセキュリティ プロトコルによっては暗号化などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA 認証の設定は、まず認証方式の名前付きリストを定義し、そのあと各種インターフェイスにそのリストを適用することで行います。
- 認可 — ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。

  RADIUS や TACACS+ などのリモート セキュリティ サーバでは、権限が定義された AV のペアを適切なユーザに関連付けることにより、所定の権限をユーザに許可します。AAA 認可は、ユーザの実行可能な内容を指定したアトリビュートをまとめることで機能します。これらのアトリビュートとデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。
- アカウンティング — ユーザ識別、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数などといったセキュリティ サーバ情報の収集と送信を行い、課金、監査、およびレポートに使用する手段を提供します。アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

（注）　認証は AAA と別個に設定することができます。ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

AAA の設定手順については、第 2 章「AAA の設定」を参照してください。

RADIUS および TACACS+ セキュリティ プロトコル

AAA は、セキュリティ機能の管理にセキュリティ プロトコルを使用します。ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

このマニュアルでは、次のセキュリティ サーバ プロトコルを設定する手順を説明します。

- RADIUS — 不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。RADIUS は AAA を使用して実装されます。シスコの実装では RADIUS クライアントはシスコ製ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。
- TACACS+ — ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ は AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。TACACS+ は独立したモジュール型の認証、許可、およびアカウンティング機能を備えています。

RADIUS の設定手順については、第 3 章「RADIUS の設定」を参照してください。TACACS+ の設定手順については、第 4 章「TACACS+ の設定」を参照してください。

SSH および Telnet

Secure Shell（SSH; セキュア シェル）サーバを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。SSH は認証に強化暗号化を使用します。Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用ができます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。

SSH および Telnet の設定手順については、第 5 章「SSH および Telnet の設定」を参照してください。

ユーザ アカウントおよびユーザ ロール

ユーザ アカウントの作成および管理を行い、NX-OS デバイス上で実行できる操作を制限するロールを割り当てることができます。Role-Based Access Control（RBAC; ロール ベース アクセス コントロール）を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

ユーザ アカウントおよび RBAC の設定手順については、第 6 章「ユーザ アカウントおよび RBAC の設定」を参照してください。

802.1X

802.1X では、クライアント サーバ ベースのアクセス制御と認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

802.1X アクセス制御では、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックをポート経由で送受信することができます。

802.1X の設定手順については、第 7 章「802.1X の設定」を参照してください。

NAC

Network Admission Control（NAC）を使用すると、エンドポイント装置にネットワーク アクセスを許可する前に、エンドポイント装置のセキュリティ適合性と脆弱性をチェックできます。このセキュリティ適合性のチェックのことを、*ポスチャ検証*といいます。ポスチャ検証により、ワーム、ウイルス、およびその他の不正アプリケーションがネットワーク全体に拡散することを防止できます。

NAC は、エンドポイント装置がネットワークの保護された領域にアクセス可能になる前に、エンドポイント装置のポスチャ（状態）がセキュリティ ポリシーに適合しているかどうかを検証します。セキュリティ ポリシーに適合する場合は、ネットワークの保護されたサービスにアクセスすることが許可されます。セキュリティ ポリシーに適合しない場合は、修復専用のネットワークにアクセスが制限されます。修復ネットワークでは装置のポスチャが再度チェックされます。

NAC の設定手順については、第 8 章「NAC の設定」を参照してください。

Cisco TrustSec

Cisco TructSec セキュリティ アーキテクチャでは、trusted network 装置のクラウドを確立してセキュア ネットワークを構築します。クラウド内の各装置は、そのネイバーにより認証されます。クラウド内の装置間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。また Cisco TrustSec では、認証時に取得した装置とユーザの識別情報も使用して、パケットがネットワークに入る際にパケットの分類（カラリング）を行います。パケットの分類には、Cisco TrustSec ネットワークへの入力パケットをタギングする方法が使用されます。これにより、セキュリティ基準およびその他のポリシー基準をデータ パス別に適用する目的に合わせて適切にパケットを識別できます。このタグのことを Security Group Tag（SGT）と呼びます。エンドポイント装置が SGT に基づいてトラフィックをフィルタリングできるようになるため、ネットワークでのアクセス制御ポリシーの適用が可能になります。Cisco TrustSec では、入力タギングと出力フィルタリングを使用してアクセス制御ポリシーを適用します。

NAC の設定手順については、第 9 章「Cisco TrustSec の設定」を参照してください。

IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。ルールには、パケットがルールと一致するために必須な条件セットを指定します。NX-OS ソフトウェアがパケットに IP ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、NX-OS デバイスは適切なデフォルト ルールを適用します。NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

IP ACL の設定手順については、第 10 章「IP ACL の設定」を参照してください。

MAC ACL

MAC（メディア アクセス制御）ACL は各パケットのレイヤ 2 ヘッダーの情報を使用してトラフィックをフィルタリングする ACL です。ルールには、パケットがルールと一致するために必須な条件セットを指定します。NX-OS ソフトウェアがパケットに MAC ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、NX-OS デバイスは適切なデフォルト ルールを適用します。NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

MAC ACL の設定手順については、第 11 章「MAC ACL の設定」を参照してください。

VACL

VLAN ACL（VACL）は、MAC ACL または IP ACL のアプリケーションの 1 つです。VLAN に出入りするすべてのパケットまたは VLAN 内でブリッジされるすべてのパケットに VACL を適用できます。VACL は、必ずセキュリティ パケット フィルタリングの用途、およびパケットを特定の物理インターフェイスにリダイレクトする用途に使用してください。VACL を方向（入力または出力）別に定義することはできません。

VACL の設定手順については、第 12 章「VLAN ACL の設定」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、限られた MAC アドレスのセットだけからのインバウンド トラフィックを許可するようにレイヤ 2 インターフェイスを設定できます。この限られた MAC アドレスのセットを、セキュア MAC アドレスといいます。さらに装置は、同じ VLAN に属する別のインターフェイス上の MAC アドレスからのトラフィックを許可しません。装置が保護できる MAC アドレスの数は、インターフェイスごとに設定できます。

ポート セキュリティの設定手順については、第 13 章「ポート セキュリティの設定」を参照してください。

DHCP スヌーピング

DHCP スヌーピングは、信頼しないホストと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。DHCP スヌーピングでは以下のアクティビティを実行します。

- 信頼しない送信元から受信した DHCP メッセージを検証し、無効なメッセージをフィルタリングします。
- DHCP スヌーピング バインディング データベースを構築し維持します。このデータベースには、リースされた IP アドレスを持つ信頼できないホストに関する情報が含まれます。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DAI（ダイナミック ARP インスペクション）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。

DHCP スヌーピングの設定手順については、第 14 章「DHCP スヌーピングの設定」を参照してください。

DAI

DAI を使用することで、有効な ARP 要求と応答だけが中継されることを保証できます。DAI がイネーブルになり適切に設定されている場合、NX-OS デバイスは次のアクティビティを実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI は DHCP スヌーピング バインディング データベースに保存された有効な IP アドレスと MAC アドレスのバインディングに基づき、ARP パケットの有効性を判断できます。このデータベースは、VLAN と装置上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。ARP パケットを信頼できるインターフェイス上で受信した場合は、装置はこのパケットを検査せずに転送します。信頼できないインターフェイス上では、装置は有効性を確認できたパケットのみを転送します。

DAI の設定手順については、第 15 章「DAI の設定」を参照してください。

IP ソース ガード

IP ソース ガードはインターフェイス単位のトラフィック フィルタです。このフィルタでは、各パケットの IP アドレスと MAC アドレスが IP と MAC アドレス バインディングの次の 2 つのいずれかのエントリと一致する場合にのみ IP トラフィックを許可します。

- DHCP スヌーピング バインディング テーブル内のエントリ
- ユーザが設定するスタティック IP ソース エントリ

信頼できる IP と MAC アドレス バインディングに基づいてフィルタリングするので、有効なホストの IP アドレスのスプーフィングを使用した攻撃の防止に役立ちます。攻撃者が IP ソース ガードを免れるには、有効なホストの IP アドレスと MAC アドレスの両方をスプーフィングしなければなりません。

IP ソース ガードの設定手順については、第 16 章「IP ソース ガードの設定」を参照してください。

キーチェーン管理

キーチェーン管理を使用すると、キーチェーンの作成と管理を行えます。キーチェーンは鍵のシーケンスを意味します（共有秘密ともいいます）。キーチェーンは、他の装置との通信を鍵ベース認証を使用して保護する機能と合わせて使用できます。装置では複数のキーチェーンを設定できます。

鍵ベース認証をサポートするルーティング プロトコルの中には、キーチェーンを使用してヒットレス キー ロールオーバーによる認証を実装できるものがあります。

キーチェーン管理の設定手順については、第 17 章「キーチェーン管理の設定」を参照してください。

トラフィック ストーム制御

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信トラフィックのレベルを 1 秒より大きなインターバルで監視できます。このインターバルの間、トラフィック レベル（ポートの合計利用可能帯域幅の割合）が、ユーザの設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックがポートに設定されたトラフィック ストーム制御レベルに達すると、トラフィック ストーム制御によりトラフィックはインターバルが終了するまでドロップされます。

トラフィック ストーム制御の設定手順については、第 18 章「トラフィック ストーム制御の設定」を参照してください。

ユニキャスト RPF

ユニキャスト Reverse Path Forwarding（RPF）機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IP ソース アドレスが注入されて引き起こされる問題を、裏付けのない IP ソース アドレスを廃棄する方法により緩和します。たとえば、スマーフィングや Tribal Flood Network（TFN）攻撃などに代表される多くの DoS 攻撃（サービス拒絶攻撃）は、ソース IP アドレスを偽造したりソース IP アドレスを頻繁に変える方法を利用し、攻撃が特定されたりフィルタリングされないように妨害しようとします。ユニキャスト RPF では、有効で、かつ IP ルーティング テーブルと一致するソース アドレスを持つパケットのみを転送することで攻撃をそらします。

ユニキャスト RPF の設定手順については、第 19 章「ユニキャスト RPF の設定」を参照してください。

CoPP

NX-OS デバイスは、DoS 攻撃によるパフォーマンスへの影響を防ぐために Control Plane Policing（CoPP; コントロール プレーン ポリシング）を備えています。NX-OS デバイスのスーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザ モジュールの動作が途絶するような場合には、重大なネットワークの停止につながります。スーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。スーパーバイザ モジュールへの攻撃には、DoS 攻撃のようにコントロール プレーンを流れる IP トラフィック ストリームが非常に高いレートで発生するものなど、さまざまな種類があります。攻撃によってコントロール プレーンはこれらのパケットの処理に大量の時間を費やしてしまい、本来のトラフィック処理が不可能になります。

CoPP の設定手順については、第 20 章「CoPP の設定」を参照してください。

レート制限

レート制限を行うことで、出力例外のリダイレクト パケットにより NX-OS デバイス上のスーパーバイザ モジュールに過剰な負荷がかかるのを回避できます。

レート制限の設定手順については、第 21 章「レート制限の設定」を参照してください。