セキュリティの概要

この章の内容は、次のとおりです。

ユーザ アカウント

Cisco Nexus 1000V へのアクセスは、各ユーザに許可される特定のアクションを定義するユーザ アカウントを設定することで実現されます。 ユーザ アカウントは最大 256 個作成できます。 管理者は、各ユーザ アカウントに対して、ロール、ユーザ名、パスワード、および有効期限を定義します。

仮想サービス ドメイン

Virtual Service Domain（VSD; 仮想サービス ドメイン）を利用すると、ネットワーク サービスのためのトラフィックの分類と分離が可能になります。このネットワーク サービスの例としては、ファイアウォールやトラフィック監視があり、その他にコンプライアンス目標（たとえばSarbanes Oxley）の達成支援のためのサービスなどがあります。

認証、許可、アカウンティング（AAA）

AAA（トリプル A と呼ばれます）は、3 つの独立した、一貫性のあるモジュラ型のセキュリティ機能を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、および暗号化（選択したセキュリティ プロトコルに基づく）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 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。
- 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 サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。 AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。 これらの属性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 ID、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信を行う手段を提供します。 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。

RADIUS セキュリティ プロトコル

AAA は、ネットワーク アクセス サーバと RADIUS セキュリティ サーバ間の通信を確立します。RADIUSは、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、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Cisco 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+ セキュリティ プロトコル

AAA は、ネットワーク アクセス サーバと TACACS+ セキュリティ サーバ間の通信を確立します。

TACACS+ は、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、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+ は独立したモジュラ型の認証、許可、アカウンティング機能を提供します。

SSH

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 は強化暗号化を使用して認証を行います。 SSH サーバは、市販の一般的な SSH クライアントとの相互運用が可能です。

SSH クライアントは、市販の一般的な SSH サーバと連動します。

Telnet

Telnet プロトコルは、ホストとの TCP/IP 接続を確立するのに使用できます。 Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、デバイス間でキーストロークをやり取りできます。 Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

アクセス コントロール リスト（ACL）

ACL は、トラフィックをフィルタリングするための順番に並べられた一連のルールです。デバイスは、パケットを適用する ACL を決定する際に、パケットをルールに対してテストしていきます。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するルールがない場合は、そのデバイスでのデフォルト ルールが適用されます。デバイスは、許可されたパケットは処理し、拒否されたパケットは廃棄します。

ACL は、ネットワークおよび特定のホストを不必要なトラフィックや望ましくないトラフィックから保護します。 たとえば、高セキュリティ ネットワークからインターネットへの HTTP トラフィックを禁止することができます。 ACL では、サイトの IP アドレスを使用して IP ACL 内でサイトを識別することにより、特定のサイトへの HTTP トラフィックだけを許可するといったこともできます。

ポート セキュリティ

ポート セキュリティを使用すると、限定的なセキュア MAC アドレス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することができます。 セキュアな MAC アドレスからのトラフィックは、同じ VLAN 内の別のインターフェイス上では許可されません。 「セキュア」にできる MAC アドレスの数は、インターフェイス単位で設定します。

DHCP スヌーピング

DHCP スヌーピングとは、DHCP サーバになりすました悪意あるホストによって IP アドレス（および関連する設定）が DHCP クライアントに割り当てられるのを防ぐためのメカニズムです。 さらに、DHCP スヌーピングには、DHCP サーバに対するある種の DoS 攻撃を防止する働きもあります。

DHCP スヌーピングを使用するには、ポートの信頼状態を設定する必要があります。この設定を使用して、信頼できる DHCP サーバと信頼できない DHCP サーバが区別されます。

さらに、DHCP スヌーピングは、DHCP サーバによって割り当てられた IP アドレスを学習するようになっているので、インターフェイスへの IP アドレスの割り当てに DHCP が使用されるときに、他のセキュリティ機能（たとえば、ダイナミック ARP インスペクションや IP ソース ガード）を機能させることができます。

ダイナミック ARP インスペクション

ダイナミック ARP インスペクション（DAI）とは、有効な ARP 要求と応答だけが中継されるようにするための機能です。信頼できないポート上でのすべての ARP 要求と応答は、この機能によって代行受信されます。代行受信されたパケットが有効な IP-to-MAC アドレス バインディングを持つことが検証されると、ローカル ARP キャッシュが更新されるか、適切な宛先にパケットが転送されます。 この機能がイネーブルのときは、無効な ARP パケットはドロップされます。

IP ソース ガード

IP ソース ガードとは、インターフェイス単位のトラフィック フィルタです。パケットの IP アドレスと MAC アドレスが、次に示す 2 つの送信元のいずれかに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 バインディング内の IP アドレスと MAC アドレス
- 管理者が設定したスタティック IP ソース エントリ