



CHAPTER 1

セキュリティの概要

この章では、Cisco Nexus 1000V で使用される次のセキュリティ機能の概要について説明します。

- 「ユーザ アカウント」 (P.1-1)
- 「仮想サービス ドメイン」 (P.1-1)
- 「認証、許可、アカウンティング (AAA)」 (P.1-2)
- 「RADIUS セキュリティ プロトコル」 (P.1-2)
- 「TACACS+ セキュリティ プロトコル」 (P.1-2)
- 「SSH」 (P.1-3)
- 「Telnet」 (P.1-3)
- 「アクセス コントロール リスト (ACL)」 (P.1-3)
- 「ポート セキュリティ」 (P.1-3)
- 「DHCP スヌーピング」 (P.1-4)
- 「ダイナミック ARP インスペクション」 (P.1-4)
- 「IP ソース ガード」 (P.1-4)

ユーザ アカウント

Cisco Nexus 1000V にアクセスするには、ユーザ アカウントをセットアップする必要があります。このユーザ アカウントによって、各ユーザに許可される具体的なアクションが定義されます。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。ユーザ アカウントの設定および管理の方法については、[第 2 章「ユーザ アカウントの管理」](#)を参照してください。

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。VSD の設定および管理の方法については、[第 3 章「VSD の設定」](#)を参照してください。

認証、許可、アカウントング (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。

- アカウントング: 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。アカウント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4章「AAA の設定」を参照してください。

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 ルータ上で稼動します。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。

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

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行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動する 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、およびアカウントング機能を提供します。

TACACS+ の設定手順については、第6章「TACACS+ の設定」を参照してください。

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 は認証に強化暗号化を使用します。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。

詳細については、[第 7 章「SSH の設定」](#)を参照してください。

Telnet

Telnet プロトコルは、ホストとの TCP/IP 接続を確立するために使用できます。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、リモート装置アドレスとして IP アドレスまたはドメイン名のいずれかを使用できます。詳細については、[第 8 章「Telnet の設定」](#)を参照してください。

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ルールを順序化したリストです。デバイスは、ある ACL がパケットに適用されると判断すると、そのルールと照合してパケットをテストします。最初に一致したルールによって、そのパケットを許可するか拒否するかが決まります。一致するものがなければ、デバイスはデフォルトのルールを適用します。デバイスは、許可されたパケットを処理し、拒否されたパケットはドロップします。

ACL により、不必要なトラフィックまたは望ましくないトラフィックからネットワークや特定のホストが保護されます。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。また、ACL は特定サイトへの HTTP トラフィックだけを許可することもできます。その場合、IP ACL 内で目的のサイトを識別するために、そのサイトの IP アドレスを使用します。

詳細については、次を参照してください。

- [第 9 章「IP ACL の設定」](#)
- [第 10 章「MAC ACL の設定」](#)

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。

詳細については、[第 11 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。

詳細については、第 12 章「[DHCP スヌーピングの設定](#)」を参照してください。

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。

詳細については、第 13 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

詳細については、第 14 章「[IP ソース ガードの設定](#)」を参照してください。