



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, 1 ページ
- 認証、許可、アカウントティング (AAA) , 1 ページ
- RADIUS セキュリティ プロトコル, 2 ページ
- TACACS+ セキュリティ プロトコル, 2 ページ
- SSH, 3 ページ
- Telnet, 3 ページ
- アクセス コントロール リスト, 3 ページ
- ポート セキュリティ, 3 ページ
- DHCP スヌーピング, 4 ページ
- ダイナミック ARP インスペクション, 4 ページ
- IP ソース ガード, 4 ページ

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。

認証、許可、アカウントティング (AAA)

認証、許可、アカウントティング (AAA) 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нта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ィール、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

セキュア シェル (SSH) 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

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。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco NX-OS ソフトウェアがパケットに IPACL 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、Cisco NX-OS ソフトウェアは適切なデフォルトルールを適用します。Cisco 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

MAC 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。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco 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、Cisco NX-OS ソフトウェアは適切なデフォルトルールを適用します。Cisco 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。

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