

目次

- [概要](#)
- [前提条件](#)
- [要件](#)
- [使用するコンポーネント](#)
- [表記法](#)
- [WLC でのトラフィック処理](#)
- [トラフィックの制御](#)
- [管理アクセスの制御](#)
- [CPU ACL](#)
- [例](#)
- [CPU ACL 適用前のテスト](#)
- [CPU ACL 適用後のテスト](#)
- [厳密な CPU ACL](#)
- [コントロールプレーン ポリシング](#)
- [HTTP トラフィックの強力な暗号化](#)
- [セッション制御](#)
- [Telnet/SSH 設定](#)
- [コンソール ポート](#)
- [要約](#)
- [セキュリティ上の実践事項](#)
- [関連情報](#)

概要

このドキュメントでは、ワイヤレス LAN コントローラ (WLC) とそれが接続されているネットワークとの間でのセキュリティの相互作用を処理するために必要な、いくつかの重要な点についてその概要を説明します。このドキュメントでは主にトラフィック制御についてとりあげるため、WLAN のセキュリティ ポリシー、AAA または WPS については扱いません。

宛先とのトラフィックに影響を及ぼすトピックが。コントローラにか。この資料でカバーされて、トラフィックに関係していないし関連しているか。ネットワークへのユーザが。

注このドキュメント内の例の一部には、誤って適用されるとコントローラへの管理アクセスに障害が発生する場合がありますため、変更を加える場合はネットワークに適用する前に検証してください。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WLC と Lightweight アクセス ポイント (LAP) の基本動作のための設定方法に関する知識
- OSI モデルの基本的な知識
- アクセス コントロール リスト (ACL) の仕組みに関する理解

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

• ファームウェア 4.2.130.0, 5.2.157.0 以降が稼働する Cisco 2000/2100/4400 シリーズ WLC
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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

[表記法](#)

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

[WLCでのトラフィック処理](#)

ネットワークセキュリティ上の重要なコンポーネントの1つはトラフィック制御です。どんな環境においても、セキュリティ問題（DoS、情報損失、権限昇格など）を未然に防ぐため、デバイスに到着するトラフィックのいくつかのタイプをブロックすることは非常に重要です。

WLCでは、トラフィック制御はある重要な事実に影響を受けます。デバイス内にはトラフィックを処理する2つのコンポーネントがあるということです。

- CPU か。すべての管理アクティビティ、RRM、LWAPP 制御、認証、DHCPなどを扱うメインのプロセッサ。
- NPU か。認証されたクライアントに対する高速トラフィック転送（有線からワイヤレス、またその逆）を処理するネットワークプロセッサ。

このアーキテクチャによって高速トラフィック転送が実現でき、メインCPUの負荷が削減されます。そのためCPUは、すべてのリソースを高レベルタスクに集中できます。

このアーキテクチャは、4400、WiSM、および3750統合コントローラで採用されています。2106およびNM-WLCと関連コントローラでは、転送はソフトウェアと、メインCPUによって実行されます。その結果、CPUを大量に消費します。これらのプラットフォームがユーザやAPを少ししかサポートできないのはそのためです。

[トラフィックの制御](#)

WLCを通るトラフィックをフィルタリングする場合、それがユーザからネットワークへのトラフィックなのか、それともメインCPUへのものなのか知ることは重要です。

- CPUへのあらゆるトラフィックに関しては、たとえば、RadiusまたはDHCPのようなSNMP、HTTPS、SSH、Telnet、またはネットワークサービスプロトコルのような管理プロトコルは、aを使用しますか。CPU ACLか。
- EoIPトンネルを通過するトラフィック（ゲストアクセス）も含め、ワイヤレスクライアントとの間で送受信されるトラフィックには、Interface ACL、WLAN ACL、またはユーザごとのACLを使用します。

トラフィックは定義されますか。CPUにか、トラフィックとして管理IPアドレスに宛先、動的インターフェイスの何れかまたはサービスポートアドレスを持つコントローラを、入力している。APマネージャは、LWAPP/CAPWAP以外のトラフィックは扱いません。

管理アクセスの制御

WLCs に a がありますか。セッションは水平になりますか。管理プロトコルのためのアクセスコントロール。コントローラで何が許可され、何が許可されないかを正しく把握するためにこの仕組みを理解することが重要です。

どの管理プロトコルが許可されるかを制限するコマンドは次のとおりです (グローバル スコープ)。

- **config network ssh enable|ディセーブル**か。これはコントローラの SSH サービスを有効にするか、またはディセーブルにします。このコマンドはデフォルトで有効になっています。無効の場合、ポート (TCP 22) にアクセスすることはできません。
- **config network telnet enable|ディセーブル**か。これはコントローラの telnet サービスを有効にするか、またはディセーブルにします。これは、デフォルトでは無効になっています。無効の場合、ポート (TCP 23) にアクセスすることはできません。
- **config network http enable|ディセーブル**か。これはコントローラの http サービスを有効にするか、またはディセーブルにします。ポート (TCP 80) にアクセスできなくなります。これは、デフォルトでは無効になっています。
- **config network https enable|ディセーブル**か。これはコントローラの https サービスを有効にするか、またはディセーブルにします。このコマンドはデフォルトで有効になっています。無効の場合、ポート (TCP 443) にアクセスすることはできません。
- **config snmp version v1|v2|v3 enable|ディセーブル**か。これはコントローラの SNMP サービスの特定のバージョンを有効にするか、またはディセーブルにします。ACL を使用していなければ、コントローラへの SNMP アクセスを防ぐためにすべて無効にする必要があります。
- **config network mgmt-via-wireless enable|ディセーブル**か。これはこのコントローラに関連付けられるクライアントがそれにアクセス管理プロトコルできること防ぎます (ssh、https、等)。ワイヤレス デバイスを考慮し、TCP 対応ポートを防御したり閉じたりはしません。つまり、この設定が無効になっている場合、ワイヤレス デバイスは、プロトコルが有効であれば SSH 接続を開けるということです。ユーザには、SSH デーモンによって生成されたユーザ名プロンプトが表示される場合がありますが、ユーザ名を入力しようとするとすぐにセッションは閉じられます。
- **config network mgmt-via-dynamic-interface enable|ディセーブル**か。これはコントローラと同じ VLAN のデバイスがそれにその VLAN の対応した 動的インターフェイス アドレスにアクセス管理プロトコル (ssh、https、等) できること防ぎます。デバイスを考慮し、TCP 対応ポートを防御したり閉じたりはしません。つまり、この設定が無効になっている場合、デバイスは、プロトコルが有効であれば SSH 接続を開けるということです。ユーザには、SSH デーモンによって生成されたユーザ名プロンプトが表示される場合がありますが、ユーザ名を入力しようとするとすぐにセッションは閉じられます。さらに、CPU ACL が設定されていない場合、ダイナミック インターフェイス VLAN から管理アドレスへのアクセスは常に可能になります。

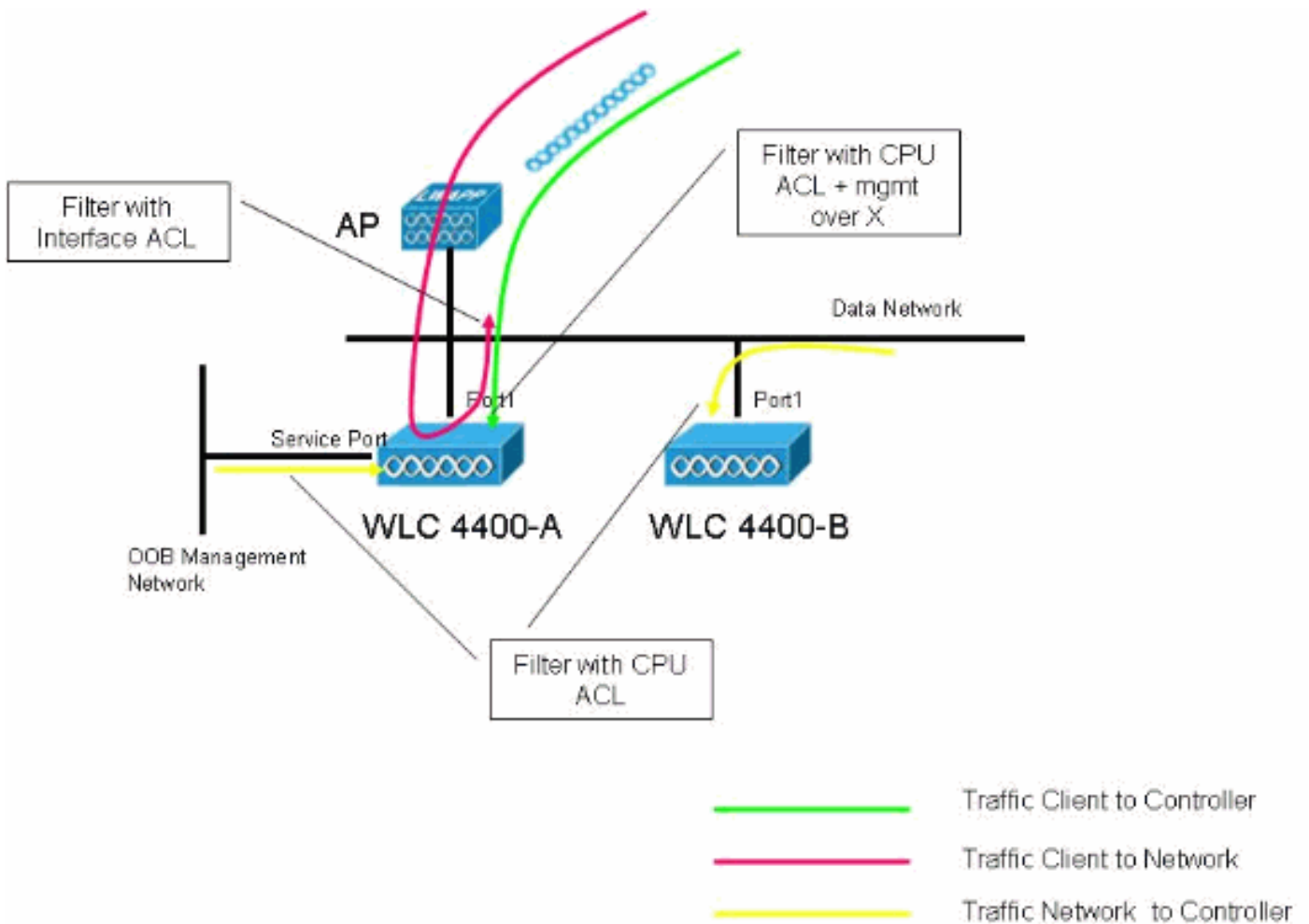
次に上記の情報に基づく設定例を示します。

次のような結果となります。

- Telnet および HTTP は使用できなくなるため、コントローラとのすべてのインタラクティブな管理トラフィックは HTTPS/SSH (暗号化) 経由で実行されます。
- このコントローラに関連付けられたワイヤレス ユーザは管理アクセス権限を取得できません

- 。このコントローラに関連付けられたワイヤレスユーザがポートスキャンを実行した場合、管理アクセスが許可されていない場合でも、SSH および HTTP はオープンとして示されます。
- 有線ユーザ (ダイナミック インターフェイスと同じ VLAN) がポートスキャンを実行した場合管理アクセスが許可されていない場合でも、SSH および HTTP はオープンとして示されません。

同じモビリティグループに複数のコントローラがある環境では、ワイヤレスクライアントは現在関連付けられたコントローラとのみ関係があります。そのため、1つのクライアントがコントローラ A と関連付けられている場合、同じモビリティグループ上のコントローラ B に対しては、このクライアントは VLAN/ダイナミック インターフェイスからのデバイスとなります。ワイヤレス設定において、管理について考慮することは重要です。トラフィック制限をどこに課すか、およびどのコマンドが各入カポイントに作用するかについては次の図を参照してください。



CPU ACL

メイン CPU と対話できるデバイスを制御する場合は常に CPU ACL が使用されます。これらのいくつかの特性について説明します。

- CPU ACL は、CPU に向かうトラフィックのみをフィルタリングし、CPU から出るトラフィックや CPU で生成されたトラフィックはフィルタリングしません。注バージョン 6.0 以降の WLC 5500 シリーズでは、CPU ACL は WLC から発生するトラフィックにも適用されます。他の WLC プラットフォームでは、この機能はバージョン 7.0 以降で実装されます。また、CPU ACL の作成時に [Direction] フィールドは関係ありません。
- すべてのコントローラ IP 管理およびダイナミック アドレスに対する CPU ACL を完全にサポ

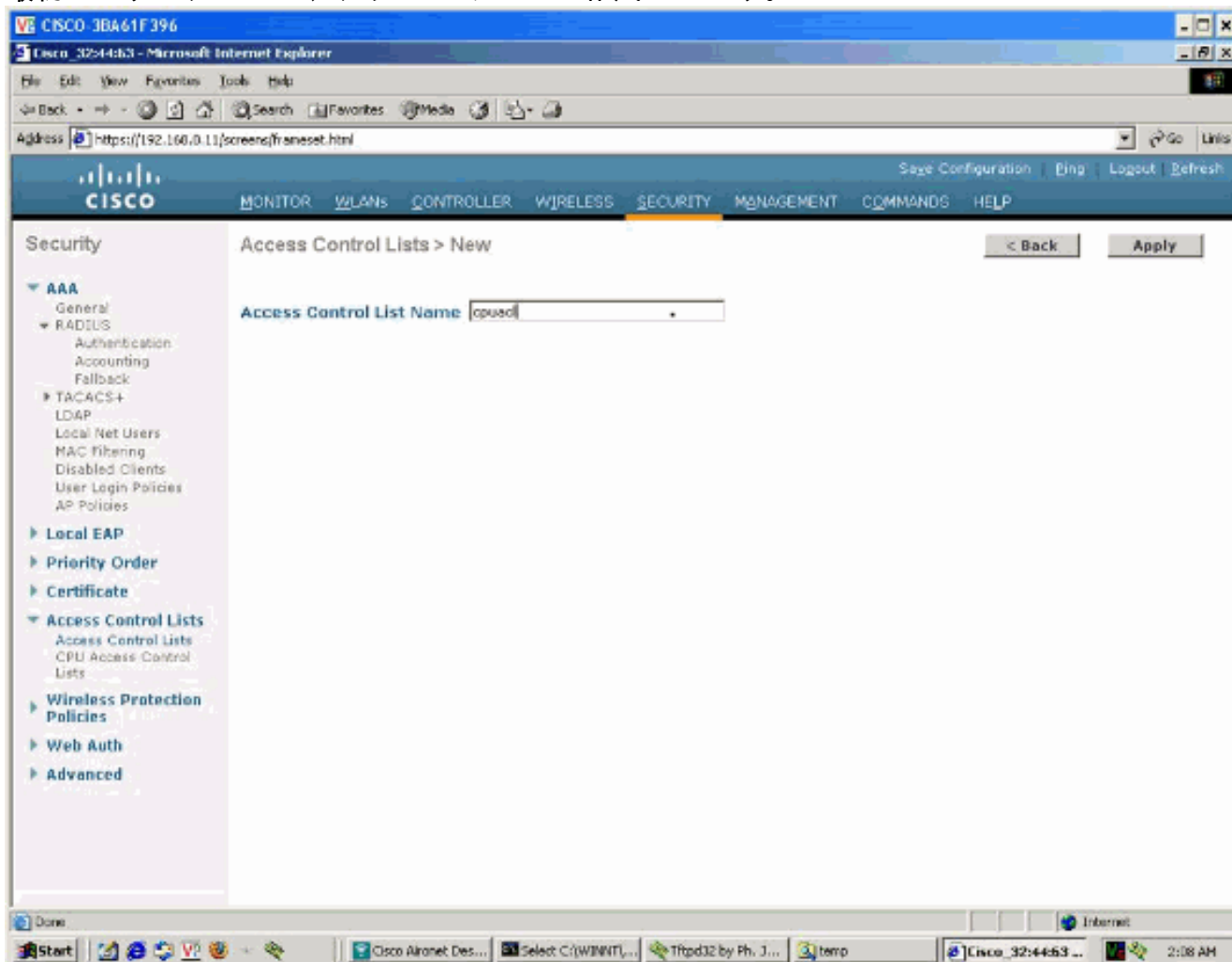
ートするのは 4.2.130.0 以降だけです。

- CPU ACL によるサービスポートトラフィックのブロッキング機能があるのは、5.0 以降だけです。
- CPU ACL を設計する場合、コントローラ間でトラフィックを制御できるようにすることは重要です。sh rules コマンドは、通常の場合で CPU ACL に許可されるトラフィックをすばやく表示できます。
- コントローラには、内部プロセス用の一連のフィルタリングルールがあり、sh rules コマンドで確認できます。これらのルールは ACL の影響を受けることはなく、すぐには変更することもできません。CPU ACL はこれらに優先されます。
- LWAPP または CAPWAP データトラフィックは、4400 ベースのコントローラ上の CPU ACL ルールから影響を受けることはありませんが、制御トラフィックは影響を受けます (厳密な ACL を実行する場合、明示的に許可する必要があります)。注 CAPWAP の制御トラフィックは CPU ACL の影響を受けません。

例

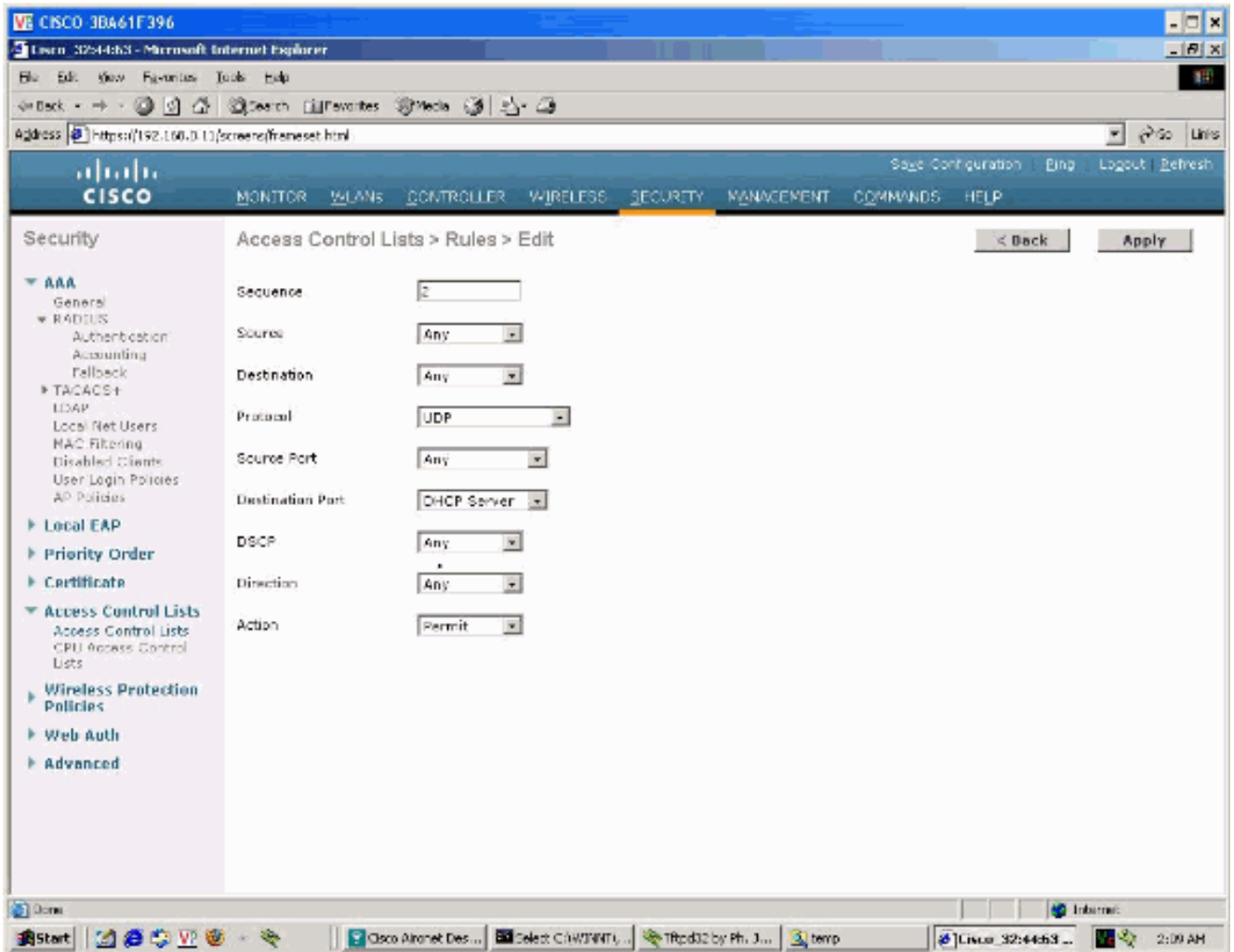
たとえば、ユーザが関連付けられていて、CPU へ向かうが、他のトラフィックも許可されている、ダイナミック インターフェイス/VLAN (192.168.20.0/24) からのすべてのトラフィックをブロックするとします。これによりワイヤレスクライアントが、DHCP との間でネゴシエートされたアドレスを取得できなくなることはありません。

1. 最初のステップとして、アクセスリストが作成されます。

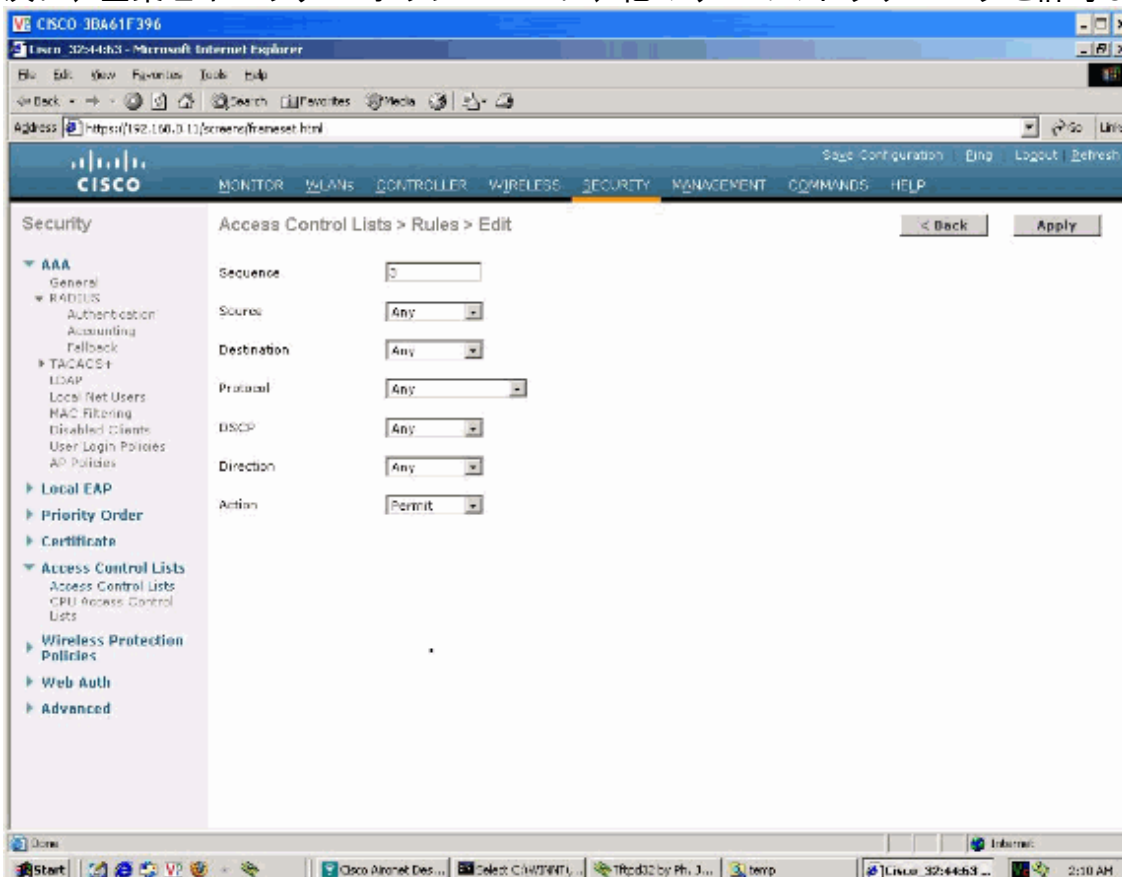


2. [Add new rule] をクリックし、送信元 192.168.20.0/24 から任意の宛先へのすべてのトラフィックをブロックするように設定します。

3. 宛先サーバポートを持つが permit アクションのない DHCP トラフィックに対して 2 番目のルールを追加します。



次に、企業セキュリティポリシーごとに、他のすべてのトラフィックを許可します。



CPU ACL 適用前のテスト

CPU ACL の効果を確認するには、関連付けられた RUN ステータスのワイヤレスクライアントからクイック スキャンを実行し、CPU ACL を適用する前に、設定に基づいて現在開かれているポートを表示します。

The screenshot shows the Zenmap application window. The target is set to 192.168.20.10 and the profile is Quick scan. The command is nmap -T4 -F 192.168.20.10. The scan results are displayed in the Nmap Output pane.

Hosts: 192.168.20.10

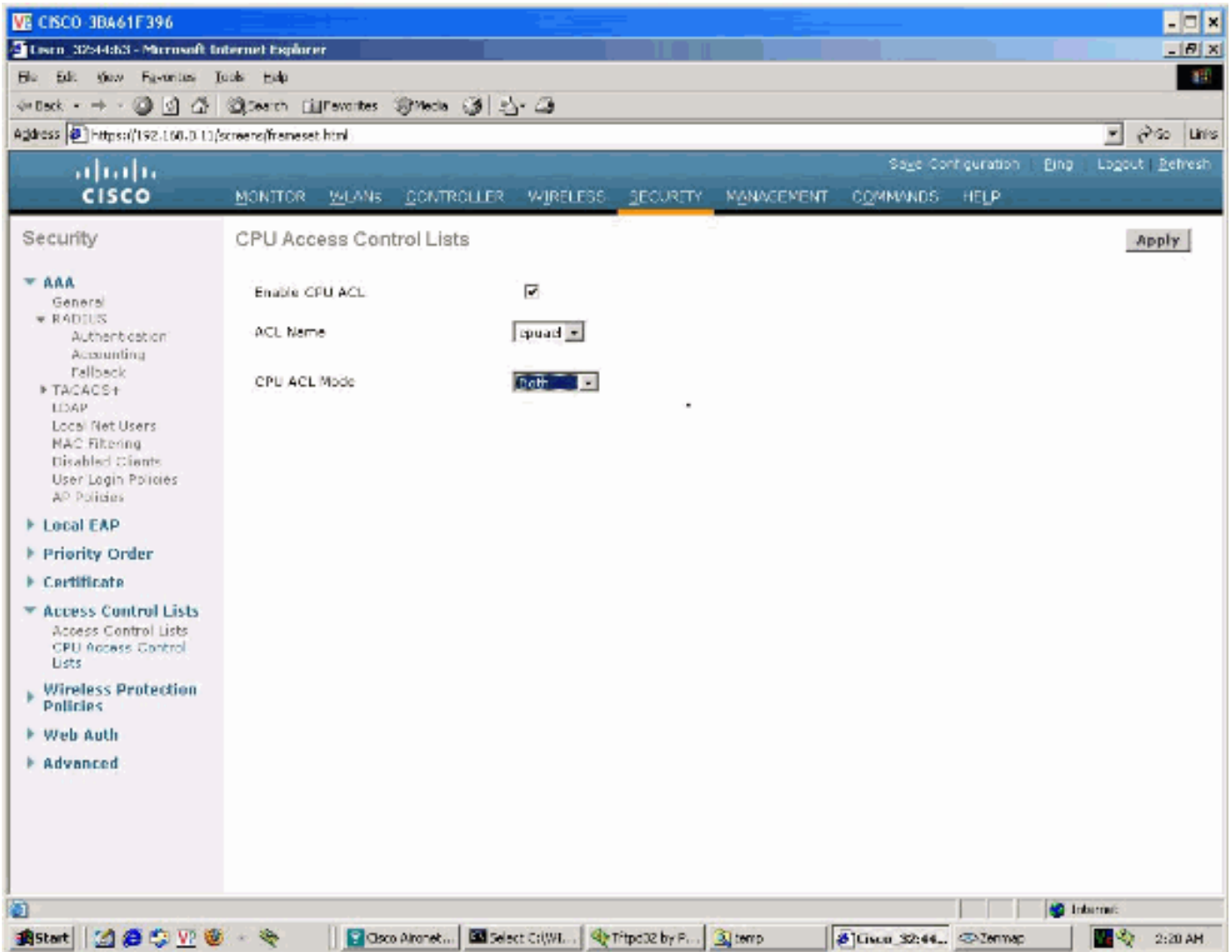
Nmap Output: nmap -T4 -F 192.168.20.10

```
Starting Nmap 4.76 ( http://nmap.org ) at
2009-02-02 02:17 Pacific Standard Time
Interesting ports on 192.168.20.10:
Not shown: 98 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
MAC Address: 00:1E:F7:32:44:67 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in
2.00 seconds
```

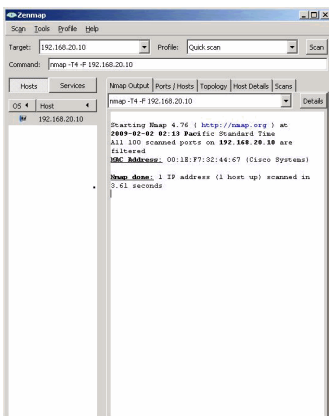
CPU ACL 適用後のテスト

[Security] > [Management] > [CPU Access Control List] に移動します。 [Enable CPU ACL] をクリックし、すでに作成した ACL を選択します。 次に、ワイヤレスクライアント、およびダイナミックインターフェイス VLAN 上の他のデバイスからのトラフィックに確実に適用されるようになるため、方向に [Both] を選択します。



注7.0 以降のすべての WLC プラットフォームの CPU ACL トラフィックには方向がなく、あるのは 6.0 の WLC5500 だけです。

先に使用したのと同じスキャンを実施した場合、コントローラのすべてのポートは閉じられていると表示されます。



厳密な CPU ACL

セキュリティポリシーが a を要求すればか。否定して下さいか。最後にポリシーのための行として、DHCP プロキシモード (デフォルト) のコントローラがそれ自身に処理のための宛先 UDP 1067 とのトラフィックを生成できるところに特に DHCP ことを RRM のための同じモビリティグループのコントローラ、モビリティおよび他のタスクの間で送信される複数のトラフィックの種類があること、そしてトラフィックをそれ自身にいくつかのオペレーションのためのコントローラによって proxied もらうかもしれませんことを理解しておくことは重要です。

デフォルトの内部転送ルールで許可されるポートの完全なリストについては、`sh rules` コマンドの出力を確認してください。完全なリストの分析は、このドキュメントの対象外です。

`config acl counter start` コマンドで、どの ACL ルールがトラフィックに適用されているかを確認できます。カウンタは、`sh acl detail ACLNAME` コマンドで表示できます。

コントロールプレーンポリシング

ネットワークデバイスの保護の1つの側面は、処理可能な容量以上の管理トラフィックによってあふれてしまうことはないという点です。4.1 コードより後のすべてのコントローラで、デフォルトで有効になっているコントロールプレーンの制限があります。これは CPU 向けのトラフィックが 2 mbps を超過すると適用されます。

ビジー状態のネットワークで、実際に制限を確認することができます (たとえば、CPU への ping で廃棄されたものを監視する、など)。この機能は、`config advanced rate` コマンドで制御できます。有効または無効にするだけで、レートを設定したり、どのトラフィックを最初に処理するかを設定したりすることはできません。

通常の運用では、有効のままにしておくことをお勧めします。

HTTP トラフィックの強力な暗号化

コントローラはデフォルトで強度の強い暗号と弱い暗号の両方に対応しており、HTTPS 設定中の古いブラウザとの互換性を確保します。コントローラは、40 ビット RC4 から、56 ビット DES、AES 256 ビットに至るまで使用可能です。最も強力な暗号の選択はブラウザが実行します。

強力な暗号だけ使用されるようにするには、`config network secureweb cipher-option high enable` コマンドを使用して有効にします。これによりコントローラは、168 3DES または 128 AES より強力な暗号だけを HTTP 管理アクセスに適用します。

セッション制御

Telnet/SSH 設定

デフォルトで、コントローラは最大 5 人の同時ユーザを許可します。タイムアウトは 5 分です。これらの値を環境内で適切に設定することは重要です。無制限 (ゼロ) に設定してしまうと、ユーザがブルートフォースアタックをしかけようとした場合、コントローラに対するサービス妨害が自由にできるようになってしまいます。次にデフォルト設定の例を示します。

設計により、ワイヤレスまたはダイナミック インターフェイス経由の管理が無効になっても、デバイスはコントローラに SSH 接続できることに留意してください。これは CPU 負荷の大きいタスクであり、WLC は同時セッションの数およびこれらのパラメータを使用できる期間を制限しません。

値は `config sessions` コマンドを使用して調整できます。

コンソール ポート

シリアル ポートには、デフォルトで 5 分に設定されている個別のタイムアウト値がありますが、トラブルシューティング セッションで 0 (無制限) に変更されることがよくあります。

デフォルトの 5 分のまま使用することを推奨します。それによって、コンソール ポート上のログイン ユーザがセッションを開いたままにした場合、誰かがコントローラに物理的にアクセスし、管理アクセスを取得することを防止できます。この値は `config serial` コマンドを使用して調整できます。

要約

WLC をセキュアにするさまざまな内容を確認しましたので、次に要約を示します。

- 使用されないプロトコルを無効にするだけでなく、レイヤ 4/レイヤ 3 へのアクセスを CPU ACL で制限することで、意図した管理ステーション以外のデバイスが WLC にアクセスするのを防ぐことは重要です。
- レート制限を有効にする必要があります (デフォルトで有効)。
- CPU やメモリ リソースを使用しながら管理 IP アドレスと直接対話することで、ユーザは管理プロトコルにアクセスできるため、`management over X` コマンドでアクセスを制御するだけではセキュアなインストールはできません。

セキュリティ上の実践事項

次にセキュリティ上の実践事項の一部を示します。

- すべてのダイナミック インターフェイス VLAN またはサブネットワークからのアクセスを防ぐ CPU ACL 作成します。ただし、DHCP プロキシが有効の場合 (デフォルトで有効)、クライアントが DHCP との間でネゴシエートされたアドレスを取得できるように、サーバポート (67) への DHCP トラフィックを許可します。ダイナミック インターフェイスにパブリック IP アドレスが割り当てられている場合、不明な送信元からダイナミック インターフェイス アドレスへのすべてのトラフィックを拒否する ACL ルールを適用することをお勧めします。
- すべての ACL ルールをインバウンドまたは方向 [any] に設定し、[both] が適用されるようにマークします (有線およびワイヤレス オプション)。検証方法：
- コントロール プレーン制限を有効にします (デフォルトで有効)。検証方法：
- 常に暗号化された管理プロトコル (HTTPS、SSH) を使用してください。これはインタラクティブ管理のデフォルト設定です。認証され、暗号化された SNMP トラフィックを許可するには、SNMP V3 を有効にしなければならない場合があります。SNMP 設定に変更を加える場合、コントローラを必ずリロードしてください。検証方法を次に示します。
- HTTPS に対する高度な暗号化を有効化します (デフォルトは無効)。

- コントローラに対する HTTPS アクセスに対して、検証されたサーバ証明書 (信頼できる CA によって署名済) を設定し、デフォルトでインストールされた自己署名証明書を置き換えることをお勧めします。
- セッションおよびコンソール タイムアウトを 5 分に設定します。

[関連情報](#)

- [Lightweight アクセス ポイントに関する FAQ \(英語\)](#)
- [ワイヤレス LAN コントローラ \(WLC\) に関する FAQ](#)
- [Cisco ワイヤレス LAN コントローラ モジュールに関する Q&A](#)
- [Unified Wireless Network における Radio Resource Management \(RRM\)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)