ワイヤレス LAN コントローラ（WLC）の保護

目次

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。

「宛先がコントローラ」のトラフィックに関するトピックがこのドキュメントの対象で、「ユーザからネットワーク」のトラフィックは扱いません。

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るため、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： 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： 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 へのトラフィック、たとえば SNMP、HTTPS、SSH、Telnet などの管理プロトコル、または Radius や DHCP などのネットワーク サービス プロトコルには「CPU ACL」を使用します。
- 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。

管理 IP アドレス、ダイナミック インターフェイス、またはサービス ポート アドレスを宛先とする、コントローラに入るトラフィックは「CPU 宛」と定義されます。 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

WLC は、管理プロトコルに対して「セッション レベル」のアクセス制御を行います。 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|disable**：コントローラで SSH サービスを有効または無効にします。 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|disable**：コントローラで telnet サービスを有効または無効にします。 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|disable**：コントローラで http サービスを有効または無効にします。 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|disable**：コントローラで https サービスを有効または無効にします。 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|disable**：コントローラで SNMP の特定のバージョンを有効または無効にします。 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|disable**：このコントローラに関連付けられたクライアントが、コントローラへ管理プロトコル（ssh、https など）でアクセスすることを防ぎます。 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|disable**：コントローラと同じ VLAN 上のデバイスが、その VLAN 上の対応するダイナミック インターフェイス アドレスに管理プロトコル（ssh、https など）でアクセスするのを防ぎます。 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。

```
(Cisco Controller) >show network summary


RF-Network Name............................. 4400
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
IP/MAC Addr Binding Check .................. Enabled


(Cisco Controller) >show acl cpu

CPU Acl Name................................ NOT CONFIGURED
Wireless Traffic............................ Disabled
Wired Traffic............................... Disabled
```

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す。

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力ポイントに作用するかの例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、通常の条件で 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 の影響は受けません。

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。

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するため、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

ポリシーの最後に、セキュリティ ポリシーが [deny any] を必要とする場合、次のことを理解しておくことが重要です。すなわち、RRM、モビリティ、およびその他のタスクに対する同じモビリティ グループ上のコントローラ間で送信されるトラフィックにはいくつかのタイプがあること、また、特に DHCP のような一部の動作において、コントローラがトラフィックをコントローラ自身にプロキシしたり、DHCP プロキシ モード（デフォルト）のコントローラが、宛先 UDP 1067 を持つ、コントローラ自身に対するトラフィックを処理のために生成したりする場合がある、ということです。

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。

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

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す。

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。

```
Cisco Controller) >show serial

Serial Port Login Timeout (minutes)..... 5
Baud Rate..................................... 9600
Character Size................................ 8
Flow Control:................................. Disable
Stop Bits..................................... 1
Parity Type:.................................. none
```

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：`(Cisco Controller) >show acl cpu`

```
CPU Acl Name.............................. acl1
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

- 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：`(Cisco Controller) >show advanced rate`

```
Control Path Rate Limiting.....................  Enabled
```

- 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。`(Cisco Controller) >show network summary`

```
RF-Network Name........................... 4400
Web Mode.................................. Disable
Secure Web Mode........................... Enable
Secure Web Mode Cipher-Option High........ Enable
Secure Web Mode Cipher-Option SSLv2....... Enable
Secure Shell (ssh)........................ Enable
Telnet.................................... Disable
...
```

- 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。`(Cisco Controller) >show serial`

```
Serial Port Login Timeout (minutes)......... 5
Baud Rate................................... 9600
Character Size.............................. 8
Flow Control:............................... Disable
Stop Bits................................... 1
Parity Type:................................ none
```

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)............ 5
```

```
Maximum Number of CLI Sessions..... 5
```

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