NAC アウトオブバンド（OOB）のワイヤレス設定例

目次

概要

このドキュメントでは、Cisco Unified Wireless Network 展開のアウトオブバンド（OOB）Cisco Network Admission Control（NAC）アプライアンスのエンドポイント セキュリティを導入するための設計ガイドラインを示します。 これらのベスト プラクティスでは、Cisco Unified Wireless Network が『Enterprise Mobility 4.1 デザイン ガイド』のガイドラインに従って導入されていることを前提とします。

推奨される設計は、仮想ゲートウェイ（ブリッジ モード）と RADIUS シングル サインオンを実装した OOB の一元管理です。 ワイヤレス LAN コントローラ（WLC）は、物理的に NAC サーバに L2 隣接して配置します。 WLC はクライアントに関連付けられ、WLC はユーザを認証します。 認証が完了すると、ユーザ トラフィックは検疫 VLAN を通って WLC から NAC サーバに渡されます。 ここでは、ポスチャ アセスメントと修復プロセスが行われます。 ユーザが認証される

と、ユーザ VLAN は検疫 VLAN から WLC 内のアクセス VLAN へ変更されます。 アクセス VLAN に移動するとき、トラフィックは NAC サーバをバイパスします。

前提条件

要件

このドキュメントのコンフィギュレーションは、NAC 4.5 と WLC 5.1 リリースに限定されます。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

- NAC サーバ 3350 4.5
- NAC Manager 3350 4.5
- WLC 2106 5.1

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。

背景説明

Cisco NAC の概要

Cisco NAC は、ネットワーク インフラストラクチャを使って、ネットワーク コンピューティング リソースにアクセスしようとするすべてのデバイスがセキュリティ ポリシーに準拠するようにします。 ネットワーク管理者は、Cisco NAC アプライアンスを使用して、有線、無線、リモートのユーザとマシンを、ネットワークにアクセスする前に認証、認定、評価、および修復できます。 Cisco NAC アプライアンスは、ラップトップ、IP フォン、またはゲーム コンソールなどのネットワーク接続デバイスを認識し、ネットワークへのアクセスを許可する前に、そのデバイスがネットワーク セキュリティ ポリシーに準拠しているかを確認し、脆弱性を修正します。

推奨される設計の用語の説明は、次のとおりです。

仮想ゲートウェイ モード (ブリッジ モード)

NAC アプライアンスを仮想ゲートウェイとして設定すると、アプライアンスは管理されているクライアント サブネット上でエンド ユーザとデフォルト ゲートウェイ (ルータ) 間をつなぐブリッジとして動作します。 特定のクライアント VLAN に対して、NAC アプライアンスは信頼できないインターフェイスから信頼されるインターフェイスへトラフィックをブリッジします。 アプライアンスで信頼できない側から信頼される側にブリッジするとき、2 つの VLAN を使用します。 たとえば、ワイヤレス LAN コントローラと NAC アプライアンスの信頼できないインターフェ

イス間では、Client VLAN 110 が定義されます。 ディストリビューション スイッチ上の VLAN 110 には、ルーテッド インターフェイスまたはスイッチ仮想インターフェイス (SVI) が関連付けられていません。 VLAN 10 は、NAC アプライアンスの信頼されるインターフェイスと、クライアント サブネットのネクストホップ ルータ インターフェイス/SVI 間で設定します。 NAC アプライアンスでは、図 1-1 に示すとおり、VLAN 110 から VLAN 10 へパケットを転送するときに VLAN タグ情報を入れ替えるというマッピング ルールを設定します。 クライアントに戻るパケットについては、逆の処理を実行します。 このモードでは、信頼できない側の VLAN から信頼される側の VLAN へは BPDU が受け渡されません。 VLAN マッピング オプションは通常、保護されたクライアントとネットワークの間で NAC アプライアンスを論理的にインラインに配置した場合に選択されます。 このブリッジ オプションは、Unified Wireless 導入時の仮想ゲートウェイ モードに NAC アプライアンスを展開するとき、必ず使用します。 理由は、NAC サーバが*上位レイヤのプロトコル*を認識し、DNS や DHCP など、認証ロール内にあるネットワークへ接続が必要なプロトコルをデフォルトで明示的に許可するからです。

図 1-1 : VLAN マッピングが設定された仮想ゲートウェイ

アウトオブバンド モード

アウトオブバンド導入環境において、ユーザ トラフィックは、認証、ポスチャ アセスメント、修復でのみ NAC アプライアンスを通過する必要があります。 ユーザが認証され、すべてのポリシー チェックを通過すると、トラフィックはネットワークを通過するよう切り替えられて、NAC サーバをバイパスできるようになります。 詳細は、『Cisco NAC アプライアンス : Clean Access Manager インストレーションおよびコンフィギュレーション ガイド』の第 4 章を参照してください。

この方法で NAC アプライアンスを設定すると、WLC は NAC Manager で管理される Cisco スイッチと同様に、NAC Manager 内の管理対象デバイスとなります。 ユーザが認証され、ポスチャ アセスメントを通過すると、NAC Manager はユーザ トラフィックのタグを NAC VLAN からアクセス権限を提供するアクセス VLAN へ付け替えるよう WLC に指示します。

図 1-2 : 仮想ゲートウェイ モードで動作するアウトオブバンド モードの NAC アプライアンス

シングル サインオン

シングル サインオン (SSO) は、ユーザの介入なしに設定できるオプションで、比較的簡単に実装できます。 この機能は NAC ソリューションの VPN SSO 機能と、クライアント PC で実行される Clean Access Agent ソフトウェアとを組み合わせて実現されます。 VPN SSO は、RADIUS アカウンティング レコードを使って、ネットワークに接続された認証済みのリモート アクセス ユーザを NAC アプライアンスに通知します。 この機能は、WLAN コントローラと連携すれば、ネットワークに接続された認証済みワイヤレス クライアントを NAC サーバに自動通知するといった、似たような使い方もできます。

NAC アプライアンスを介して SSO 認証、ポスチャ アセスメント、修復、ネットワーク アクセスを実行するワイヤレス クライアントの例は、図 1-3 ~ 1-6 を参照してください。

この流れを、図 1-3 に示します。

1. ワイヤレス ユーザはアップストリーム AAA サーバに対して、WLAN コントローラを通じて 802.1x/EAP 認証を実行します。
2. クライアントは、AAA サーバまたは DHCP サーバのいずれかから IP アドレスを取得します。

3. クライアントが IP アドレスを取得すると、WLC はワイヤレス クライアントの IP アドレスを含む RADIUS アカウンティング（開始）レコードを NAC アプライアンスに転送します。**注:** WLC コントローラは、802.1x クライアント認証と IP アドレスの割り当てで 1 つの RADIUS アカウンティング レコード（開始）を使用します。一方で、Cisco Catalyst スイッチは 2 つのアカウンティング レコードを送信します。 1 つは 802.1x クライアント認証後に送信されるアカウンティング開始で、もう 1 つはクライアントに IP アドレスが割り当てられた後に送信される暫定アップデートです。
4. ネットワーク接続を検知すると、NAC Agent は（SWISS プロトコルが動作する）CAM に接続を試みます。 NAC サーバはトラフィックを傍受し、ユーザがオンライン ユーザ リストに登録されているかどうかを NAC Manager に問い合わせます。 認証されたクライアントのみがオンライン ユーザ リストに登録されます。これは、上記の例にあるとおり、手順 3 で RADIUS アップデートを実行した結果です。
5. NAC Agent はクライアント マシンのセキュリティ/リスク ポスチャに対してローカル アセスメントを実行し、NAC サーバでネットワーク アドミッションの決定ができるよう結果を渡します。**図 1-3：クライアント認証プロセスとポスチャ アセスメント**

この流れを、図 1-4 に示します。

1. NAC アプライアンスはエージェント アセスメントを NAC Appliance Manager（CAM）に転送します。
2. この例では、クライアントが準拠していないと CAM が判断し、NAC アプライアンスにユーザを検疫ロールへ入れるよう指示しています。
3. 続いて、NAC アプライアンスはクライアント エージェントに修復情報を送信します。**図 1-4 CAS から CAM にポスチャ アセスメント情報を送信**

このシーケンスは図 1-5 で起こります:

1. クライアント エージェントは、修復完了までの時間を表示します。
2. エージェントはユーザが修復プロセスを完了できるよう、順を追って説明します（たとえばアンチウイルスの定義ファイルをアップデートするなど）。
3. 修復が完了すると、エージェントは NAC サーバをアップデートします。
4. CAM にはアクセプタブル ユース ポリシー（AUP）のステートメントが表示されます。**図 1-5：CAS のクライアント修復プロセスでデバイスを強化**

このシーケンスは図 1-6 で起こります:

1. AUP を承認すると、NAC アプライアンスはユーザをオンライン（認証）ロールに切り替えます。
2. SSO 機能では、オンライン ユーザ リストにクライアントの IP アドレスを入力します。 修復後、認証リストにはホストのエントリが追加されます。 両方のテーブルは（検知されたクライアント テーブルと併せて）CAM（NAC Appliance Manager）が管理します。
3. NAC Manager は、ユーザの VLAN を検疫 VLAN からアクセス VLAN に変更できないかどうかについて、WLC に SNMP 書き込み通知を送信します。
4. アクセス VLAN タグの付いたユーザ トラフィックは、徐々に WLC から排出されます。 この特定のユーザ トラフィックでは、NAC サーバがすでにパスから外れています。**図 1-6 アクセス VLAN に切り替えられた認証クライアントは CAS をバイパス**

ワイヤレス ユーザ認証を実行する上で最も透過的な方法は、NAC サーバ上で VPN-SSO 認証を有効化して、RADIUS アカウンティングを NAC サーバへ転送するよう WLC を設定することです。 アカウンティング レコードをネットワーク内のアップストリームの RADIUS サーバに転送する必要がある場合、RADIUS サーバへアカウンティング パケットを転送するよう NAC サーバを設定することができます。

注: クライアント PC に Clean Access Agent をインストールせずに VPN-SSO 認証を有効化しても、ユーザは自動で認証されます。 ただし、Web ブラウザを開いて接続を試みるまで、NAC アプライアンスには自動接続されません。 この場合、ユーザが Web ブラウザを開くと、すぐに“エージェントレス” フェーズで (ログオン プロンプトなしで) NAC アプライアンスにリダイレクトされます。 SSO プロセスが完了すると、もともと要求していた URL へ接続されます。

NAC OOB ワイヤレス ソリューションの設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を使用してください。

これまでの NAC 導入では、WLC は Cisco NAC アプライアンスとインバンド モードのみで統合されていたため、NAC アプライアンスはユーザ認証後もデータ パスに残っていました。 NAC アプライアンスがポスチャ検証を完了すると、employee / guest はロールに従ってネットワークにアクセスできるようになりました。

NAC 4.5 と WLC 5.1 リリースになり、ワイヤレス NAC ソリューションでは NAC アプライアンスを使用した OOB 統合をサポートするようになりました。 クライアントが L2Auth を関連付けて完了すると、検疫インターフェイスが WLAN/SSID と関連付けられているかが確認されます。 関連付けられている場合、最初のトラフィックは検疫インターフェイスへ送信されます。 クライアントのトラフィック フローは、NAC アプライアンスにトランクされた検疫 VLAN に渡されます。 ポスチャ検証が完了すると、NAC Manager はアクセス VLAN ID をアップデートするための SNMP 設定メッセージを送信します。 コントローラはアクセス VLAN ID を使って自らアップデートを実行し、NAC サーバなしでデータ トラフィックをコントローラから直接ネットワークへ切り替え始めます。

図 2-1 スイッチを介してブリッジ モードで WLC に接続されたスタンドアロン CAS の例

図 2-1 では、WLC は検疫 VLAN とアクセス VLAN (176 と 175) を伝送するトランク ポートに接続されています。 スイッチでは、検疫 VLAN のトラフィックは NAC アプライアンスにトランクされており、アクセス VLAN のトラフィックはレイヤ 3 スイッチに直接トランクされています。 NAC アプライアンス上の検疫 VLAN に到達するトラフィックは、静的なマッピング設定に基づいてアクセス VLAN にマップされます。 クライアントが L2Auth との関連付けを完了すると、検疫インターフェイスと関連付けられているかが確認されます。 関連付けられている場合、データは検疫インターフェイスへ送信されます。 クライアントのトラフィック フローは、NAC アプライアンスにトランクされた検疫 VLAN に渡されます。 ポスチャ検証が完了すると、NAC サーバ (CAS) は SNMP 設定メッセージをコントローラに送信し、アクセス VLAN ID をアップデートするよう通知します。そして、データ トラフィックは NAC サーバなしでコントローラから直接ネットワークへの切り替えを開始します。

制限

- ポート プロファイルの関連付けはしない
- NAC Manager で VLAN ID を指定しない WLC で定義
- MAC フィルタ サポートではロール設定から VLAN ID を使用することはできない
- アウトオブバンド仮想ゲートウェイ NAC サーバ モードのみサポート
- WLC と NAC サーバ間のレイヤ 2 関連付け
- NAC ISR と WLC NM でワイヤレス OOB NAC を実行するよう設定することはできない

注: 仮想ゲートウェイ モードで安全に VLAN を設定する方法については、『Cisco NAC アプライ

アンス：Clean Access サーバ設定ガイド (リリース 4.8(1))』の「仮想ゲートウェイ モードでの VLAN マッピング」を参照してください。

Catalyst Switch Configuration

```
interface GigabitEthernet2/21
 description NAC SERVER UNTRUSTED INTERFACE switchport switchport trunk native vlan 998
switchport trunk allowed vlan 176 switchport mode trunk no ip address ! interface
GigabitEthernet2/22 description NAC SERVER TRUSTED INTERFACE switchport switchport trunk native
vlan 999 switchport trunk allowed vlan 11,175 switchport mode trunk no ip address ! interface
GigabitEthernet2/23 description NAC MANAGER INTERFACE switchport switchport access vlan 10 no ip
address spanning-tree portfast ! interface GigabitEthernet2/1 description WLC switchport
switchport trunk allowed vlan 75,175,176 switchport trunk native vlan 75 switchport mode trunk
no ip address ! interface Vlan75 Description WLC Management VLAN ip address 10.10.75.1
255.255.255.0 ! interface Vlan175 Description Client Subnet Access VLAN ip address 10.10.175.1
255.255.255.0 end
```

WLC および NAC Manager 上で NAC OOB を設定する手順

次の手順に従って、WLC および NAC Manager 上で NAC OOB を設定します。

1. コントローラで SNMP v2 モードを有効にします。
2. CAM Manager 上で WLC のプロファイルを作成します。 [OOB Management Profile] > [Device] > [New] をクリックします。
3. CAM でプロファイルが作成されたら、WLC をプロファイルに追加します。 [OOB Management] > [Devices] > [New] に移動したら、WLC の管理 IP アドレスを入力します。これで、コントローラは CAM Manager に追加されました。
4. WLC から CAM を SNMP トラップ レシーバとして追加します。 CAM 内のトラップ レシーバと同じ名前の SNMP レシーバを設定します。
5. コントローラで指定した名前と同じ名前で SNMP トラップ レシーバを CAM で設定します。 [OOB Management] > [SNMP Receiver] の下の [Profiles] をクリックします。この段階で、WLC と CAM の間でクライアントのポスチャ検証やアクセス/検疫状態のアップデートについて通信できるようになりました。
6. コントローラで、アクセス VLAN と検疫 VLAN を使用するためのダイナミック インターフェイスを作成します。
7. WLAN を作成してダイナミック インターフェイスと関連付けします。
8. 最後に、WLAN で NAC を有効にします。
9. CAS サーバ内のクライアント サブネットを管理対象のサブネットとして追加します。 [CAS server] > [Select your CAS server] > [Manage] > [Advanced] > [Managed Subnets] > [Add Unused IP address from the client subnet] の順にクリックして、管理対象のサブネットに検疫 VLAN (信頼できない VLAN) を設定します。
10. CAS で VLAN マッピングを作成します。 [CAS server] > [Select your CAS server] > [Manage] > [Advanced] > [VLAN Mapping] の順にクリックします。 信頼される VLAN としてアクセス VLAN を、信頼できない VLAN として検疫 VLAN を追加します。

OOB ワイヤレス ソリューションによるシングル サインオンの設定

ワイヤレス SSO を有効にするための要件は、次のとおりです。

1. NAC サーバの VPN 認証を有効にする — WLC は NAC アプライアンス内で「VPN コンセントレータ」として定義されています。”“

2. WLC で RADIUS アカウンティングを有効にする — NAC アプライアンス内で定義されたコントローラを設定し、NAC 内の管理対象サブネットである 802.1x/EAP WLAN ごとの NAC アプライアンスに対して RADIUS アカウンティング レコードを送信するようにします。

NAC Manager で SSO を設定する手順

次の手順に従って、NAC Manager で SSO を設定します。

1. CAM の左側のメニューにある [Device Management] で [CCA Server] を選択し、[NAC Server] リンクをクリックします。
2. [Server Status] ページで [Authentication] タブ、[VPN Auth] サブメニューの順に選択します。 図 3-1 を参照してください。**図 3-1：NAC サーバでシングル サインオンを有効にする**
3. [VPN Concentrators Setting]（ 図 3-2 ）を選択して WLC の新規エントリを追加します。 WLC の入力フィールドに管理 IP アドレスを入力して、WLC と NAC サーバの間で使用する共有秘密を入力します。**図 3-2：VPN コンセントレータのセクションで WLC を RADIUS クライアントとして追加する**
4. ロール マッピングについては、[User Management] > [Auth Servers] の下で、新しい認証サーバ タイプの **vpn sso** を追加します。
5. [Mapping] アイコンをクリックして、[Mapping Rule] を追加します。 マッピングは、WLC がアカウンティング パケットで送信するクラス属性 25 の値によって異なります。 この属性値は RADIUS サーバで設定し、ユーザ認証によって変更されます。 この例では、属性値は **ALLOWALL** で、ロールの **AllowAll** 内に配置されています。

ワイヤレス LAN コントローラで SSO を設定する手順

NAC サーバで SSO 機能を利用するには、WLC で RADIUS アカウンティングを設定する必要があります。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（ OIT ）（ 登録ユーザ専用 ）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

確認用の CISCO WLC CLI コマンド

```
(Cisco Controller) >show interface summary

Interface Name    Port Vlan Id    IP Address      Type    Ap Mgr Guest
------------------------------------------------ ---- -------- ------
ap-manager        1    untagged   10.10.75.3      Static  Yes    No
management        1    untagged   10.10.75.2      Static  No     No
nac-vlan          1    175        10.10.175.2     Dynamic No     No
service-port      N/A  N/A        192.168.1.1     Static  No     No
virtual           N/A  N/A        1.1.1.1         Static  No     No


(Cisco Controller) >show interface detailed management

Interface Name..................................... management
```

```
MAC Address..................................... 00:18:73:34:b2:60
IP Address...................................... 10.10.75.2
IP Netmask...................................... 255.255.255.0
IP Gateway...................................... 10.10.75.1
VLAN............................................ untagged
Quarantine-vlan................................. 0
Active Physical Port............................ 1
Primary Physical Port........................... 1
Backup Physical Port............................ Unconfigured
Primary DHCP Server............................. 10.10.75.1
Secondary DHCP Server........................... Unconfigured
DHCP Option 82.................................. Disabled
ACL............................................. Unconfigured
AP Manager...................................... No
Guest Interface................................. No

(Cisco Controller) >show interface detailed nac-vlan

Interface Name.................................. nac-vlan
MAC Address..................................... 00:18:73:34:b2:63
IP Address...................................... 10.10.175.2
IP Netmask...................................... 255.255.255.0
IP Gateway...................................... 10.10.175.1
VLAN.............................................. 175 Quarantine-
vlan.................................. 176 Active Physical Port............................ 1
Primary Physical Port........................... 1 Backup Physical
Port............................ Unconfigured Primary DHCP Server.............................
10.10.175.1 Secondary DHCP Server........................... Unconfigured DHCP Option
82................................. Disabled ACL.........................................
Unconfigured AP Manager..................................... No Guest
Interface................................. No
```

WLC GUI からクライアントのステータスを確認

クライアントは、NAC アプライアンスのポスチャ分析が完了するまで検疫状態になります。

クライアントの NAC ステータスは、ポスチャ分析が完了したら **Access** になっていなければなりません。

WLC が動作する NAC サーバでシングル サインオンを確認

[VPN Auth] から [Active Client] サブセクションに移動し、WLC からのアカウンティング開始パケットを受信したかどうか確認します。 このエントリは、クライアント マシンにインストールされた CCA エージェントとともに表示されます。

エージェントを使っていない場合は、ブラウザを開いて SSO プロセスを完了させます。 ブラウザを開くと、SSO プロセスが実行され、オンライン ユーザ リスト（OUL）にユーザが表示されます。 RADIUS アカウンティング停止パケットとともに、ユーザはアクティブ クライアント リストから削除されます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされ

ています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

関連情報

- Remote Authentication Dial-In User Service（RADIUS）
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems