H3Cアクセスコントローラ

ユーザーアクセスおよびポータル認証設定ガイド

New h3c Technologies Co., Ltd.
http://www.h3c.comhttp://www.h3c.com/

ドキュメントバージョン:6W103-20200507製品バージョン:R5426P02

内容

ポータル認証の構成

ポータル認証について

ポータル認証は、ネットワークへのユーザーアクセスを制御します。ポータルは、ユーザーがポータル認証ページに入力したユーザー名とパスワードによってユーザーを認証します。通常、ポータル認証は、アクセスレイヤーおよび重要なデータエントリに配置されます。

ポータル対応ネットワークでは、ユーザーはポータルWebサーバーによって提供される認証Webサイトにアクセスすることによって、ポータル認証をアクティブに開始できます。または、他のWebサイトにアクセスすると、認証のためにポータル認証ページにリダイレクトされます。

このデバイスは、Portal1.0、Portal2.0、およびPortal3.0をサポートします。

ポータル認証の利点

ポータル認証には、次の利点があります。

- クライアントソフトウェアをインストールしなくても、Webブラウザを介して認証を実行できます。
- ISPに対して、多様な管理オプションと拡張機能を提供します。たとえば、ISPは、コミュニティサービスを提供したり、認証ページに情報を公開したりできます。

拡張ポータル機能

拡張ポータル機能ウイルス対策ポリシーを強制的に適用することにより、拡張ポータル機能はホストがウイルスから保護するのに役立ちます。Portalでは、次の拡張機能がサポートされています。

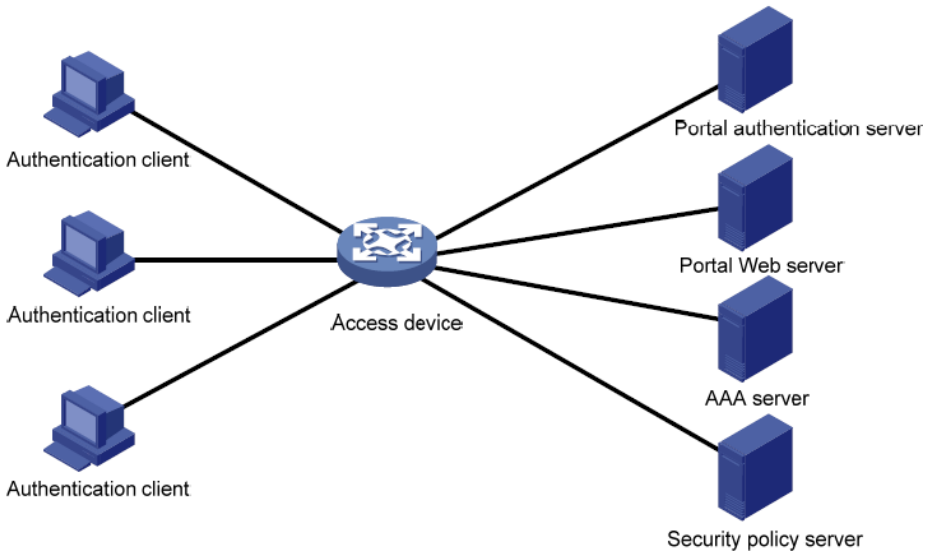
- セキュリティチェックユーザーホストがウイルス対策ソフトウェア、ウイルス定義ファイル、許可されていないソフトウェア、およびオペレーティングシステムのパッチをインストールするかどうかを、認証後に検出します。
- リソースアクセス制限認証されたユーザーが、ウイルスサーバーやパッチサーバーなどの特定のネットワークリソースにアクセスできるようにします。ユーザーはセキュリティチェックに合格すると、さらに多くのネットワークリソースにアクセスできます。

セキュリティチェックは、H3C iMCセキュリティポリシーサーバーおよびiNodeクライアントと連携する必要があります。

ポータルシステム

一般的なポータルシステムは、認証クライアント、アクセスデバイス、ポータル認証サーバー、ポータルWebサーバー、AAAサーバー、およびセキュリティポリシーサーバーという基本コンポーネントで構成されています。

図1 ポータルシステム



認証クライアント

認証クライアントは、HTTP/HTTPSを実行するWebブラウザまたはポータルクライアントを実行するユーザーホストです。ユーザーホストのセキュリティチェックは、ポータルクライアントとセキュリティポリシーサーバー間の相互作用を介して実装されます。H3C iNodeクライアントのみがサポートされます。

アクセスデバイス

アクセスデバイスはアクセスサービスを提供します。次の機能があります。

- 認証されていないユーザーのすべてのHTTPまたはHTTPS要求をポータルWebサーバーにリダイレクトします。
- ポータル認証サーバーおよびAAAサーバーと相互作用して、認証、認可、およびアカウンティングを完了します。
- ポータル認証に合格したユーザーが、許可されたネットワークリソースにアクセスできるようにします。

ポータルサーバー

ポータルサーバーとは、ポータルの認証サーバーとポータルWebサーバーの総称です。

ポータルWebサーバーは、Web認証ページを認証クライアントにプッシュし、ユーザー認証情報(ユーザー名およびパスワード)をポータル認証サーバーに転送します。ポータル認証サーバーは、認証クライアントからの認証要求を受信し、アクセスデバイスと対話してユーザーを認証します。通常、ポータルWebサーバーはポータル認証サーバーと統合されており、独立したサーバーにすることもできます。

AAAサーバー

AAAサーバーはアクセスデバイスと相互作用して、ポータルユーザーの認証、認可、アカウンティングを実装します。ポータルシステムでは、RADIUSサーバーはポータルユーザーの認証、認可、アカウンティングを実行でき、LDAPサーバーはポータルユーザーの認証を実行できます。

セキュリティポリシーサーバー

セキュリティポリシーサーバーは、ポータルクライアントおよびアクセスデバイスと対話して、ユーザーのセキュリティチェックおよび認可を行います。セキュリティポリシーサーバーと対話できるのは、ポータルクライアントを実行するホストのみです。

リモートポータルサーバーを使用したポータル認証

ポータルシステムのコンポーネントは、次のように相互作用します。

1. 認証されていないユーザーは、Webブラウザを介してインターネットWebサイトにアクセスすることによって認証を開始します。HTTPまたはHTTPS要求を受信すると、アクセスデバイスはその要求をポータルWebサーバーによって提供されるWeb認証ページ。ユーザーは認証Webサイトにアクセスしてログインすることもできます。拡張ポータル機能の場合、ユーザーはH3C iNodeクライアントを介してログインする必要があります。
2. ユーザーは、認証ページ/ダイアログボックスに認証情報を入力し、情報を送信します。ポータルWebサーバーは、情報をポータル認証サーバーに転送します。ポータル認証サーバーは、情報を処理してアクセスデバイスに転送します。
3. アクセスデバイスはAAAサーバーと相互作用して、ユーザーの認証、認可、アカウンティングを実装します。
4. セキュリティポリシーがユーザーに適用されていない場合、アクセスデバイスは認証されたユーザーにネットワークへのアクセスを許可します。

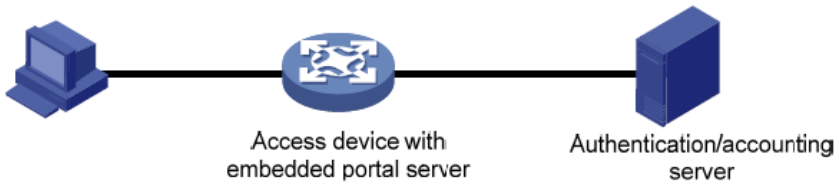
   セキュリティポリシーがユーザーに適用されている場合は、ポータルクライアント、アクセスデバイスおよびセキュリティポリシーサーバーが相互に作用してユーザーホストをチェックします。ユーザーがセキュリティチェックに合格すると、セキュリティポリシーサーバーは、チェック結果に基づいてユーザーのリソースへのアクセスを認可します。

ローカルポータルサービス

システムコンポーネント

図2に示すように、ローカルポータルシステムは、認証クライアント、アクセスデバイスおよびAAAサーバーで構成されています。アクセスデバイスはポータルWebサーバーおよびポータル認証サーバーの両方として機能し、認証クライアントにローカルポータルWebサービスを提供します。認証クライアントはWebブラウザのみであり、ポータルクライアントを実行するユーザーホストであることはできません。したがって、拡張ポータル機能はサポートされず、セキュリティポリシーサーバーは必要ありません。

図2 システムコンポーネント



ポータルページのカスタマイズ

ローカルポータルのWebサービスを提供するには、デバイスがユーザーにプッシュする一連の認証ページをカスタマイズする必要があります。複数の一連の認証ページをカスタマイズして、各一連のページを.zipファイルに圧縮し、圧縮ファイルをデバイスの記憶域メディアにアップロードできます。デバイスでは、default-logon-pageコマンドを使用して、いずれかのファイルをデフォルトの認証ページファイルとして指定する必要があります。

認証ページのカスタマイズの詳細については、「認証ページのカスタマイズ」を参照してください。

ポータル認証モード

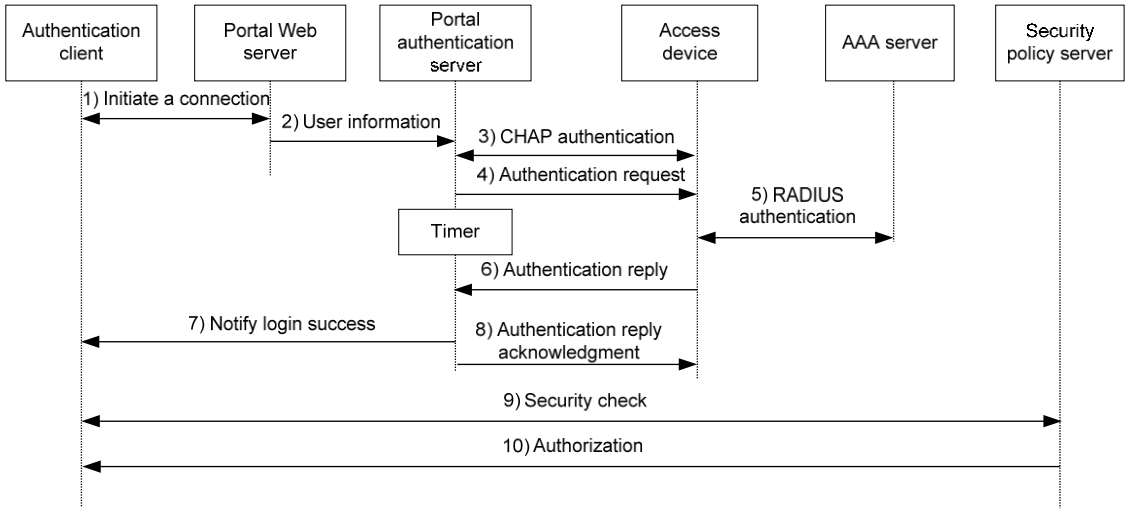
直接認証

ユーザーは、パブリックIPアドレスを手動で構成するか、DHCPを使用してパブリックIPアドレスを取得します。認証前にユーザーがアクセスできるのは、ポータルのWebサーバーおよび事前定義された認証不要のWebサイトのみです。認証を受け渡すと、ユーザーは他のネットワークリソースにアクセスできます。直接認証のプロセスは、再DHCP認証のプロセスよりも簡単です。

ポータル認証プロセス

直接認証プロセス(CHAP/PAP認証を使用)

図3 直接認証プロセス



直接認証プロセスは次のとおりです。

1. ポータルユーザーはHTTPまたはHTTPSを介してインターネットにアクセスし、HTTPまたはHTTPSパケットがアクセスデバイスに到着します。
   - パケットがポータルフリー規則に一致する場合、アクセスデバイスはパケットの通過を許可します。
   - パケットがどのポータルフリールールにも一致しない場合、アクセスデバイスはパケットをポータルWebサーバーにリダイレクトします。ポータルWebサーバーはWeb認証ページをユーザーにプッシュし、ユーザーがユーザー名とパスワードを入力できるようにします。
2. ポータルWebサーバーは、ユーザー認証情報をポータル認証サーバーに送信します。
3. ポータル認証サーバーおよびアクセスデバイスはCHAPメッセージを交換します。このステップはPAP認証ではスキップされます。ポータル認証サーバーは使用する方法(CHAPまたはPAP)を決定します。
4. ポータル認証サーバーはユーザー名とパスワードを認証要求パケットに追加してアクセスデバイスに送信します。一方、ポータル認証サーバーはタイマーを起動して認証応答パケットを待機します。
5. アクセスデバイスとRADIUSサーバーは、RADIUSパケットを交換します。
6. アクセスデバイスは、認証の成功または失敗を通知するために、認証応答パケットをポータル認証サーバーに送信します。

7. ポータル認証サーバーは、認証の成功または失敗パケットをクライアントに送信します。
8. 認証が成功すると、ポータル認証サーバーは認証応答確認パケットをアクセスデバイスに送信します。

クライアントがiNodeクライアントの場合、認証プロセスには拡張ポータル機能のステップ9とステップ10が含まれます。それ以外の場合は、認証プロセスは完了しています。

9. クライアントとセキュリティポリシーサーバーはセキュリティチェック情報を交換します。セキュリティポリシーサーバーは、ユーザーホストがウイルス対策ソフトウェア、ウイルス定義ファイル、無許可ソフトウェアおよびオペレーティングシステムパッチをインストールするかどうかを検出します。
10. セキュリティポリシーサーバーは、チェック結果に基づいてユーザーに特定のネットワークリソースへのアクセスを認可します。アクセスデバイスは認可情報を保存し、ユーザーのアクセスを制御するために使用します。

ポータルによるEAPのサポート

EAPをサポートするポータル認証を使用するには、ポータル認証サーバーおよびクライアントがH3C iMCポータルサーバーおよびH3C iNodeポータルクライアントである必要があります。ローカルポータル認証はEAP認証をサポートしていません。

ユーザー名およびパスワードベースの認証と比較して、デジタル証明書ベースの認証ではセキュリティが向上します。

Extensible Authentication Protocol(EAP)では、EAP-TLSなど、いくつかのデジタル証明書ベースの認証方法がサポートされています。EAPと連携して、ポータル認証でデジタル証明書ベースのユーザー認証を実装できます。

図4 ポータルのEAPサポート作業フロー図

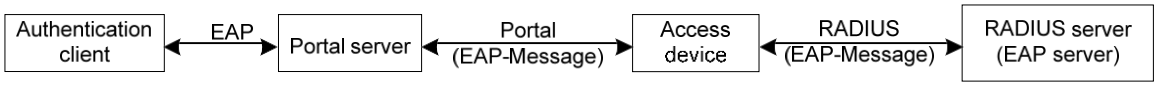


図4に示すように、認証クライアントとポータル認証サーバーはEAP認証パケットを交換します。ポータル認証サーバーとアクセスデバイスは、EAP-Message属性を伝送するポータル認証パケットを交換します。アクセスデバイスとRADIUSサーバーは、EAP-Message属性を伝送するRADIUSパケットを交換します。EAPサーバー機能をサポートするRADIUSサーバーは、EAP-Message属性にカプセル化されたEAPパケットを処理し、EAP認証結果を提供します。

アクセスデバイスはEAP-Messageアトリビュートを処理せず、ポータル認証サーバーとRADIUSサーバー間で転送するだけです。したがって、アクセスデバイスはEAP認証をサポートするための追加設定を必要としません。

ポータルフィルタリング規則

アクセスデバイスは、ポータルフィルタリング規則を使用して、ユーザートラフィック転送を制御します。

ポータルユーザーの設定および認証ステータスに基づいて、デバイスは次のカテゴリのポータルフィルタリング規則を生成します。

- 最初のカテゴリ: この規則では、ポータルWebサーバー宛てのユーザーパケットおよびポータルフリー規則に一致するパケットの通過が許可されます。
- 2番目のカテゴリ: ACLが認可されていない認証済みユーザーの場合、この規則により、ユーザー

は任意の宛先ネットワークリソースにアクセスできます。ACLが認可されている認証済みユーザーの場合、この規則により、ユーザーはACLによって許可されたリソースにアクセスできます。ユーザーがオンラインになると規則が追加され、オフラインになると規則が削除されます。

デバイスは、次のタイプの認可ACLをサポートします。

- 基本ACL(ACL2000～ACL2999)。
- 拡張ACL(ACL3000～ACL3999)。
- レイヤ2ACL(ACL4000～ACL4999)。

許可ACLを有効にするには、ACLが存在し、counting、established、fragment、source-mac、またはloggingキーワードで設定されたルールを除外するACLルールがあることを確認します。ACLルールの詳細については、『Security Command Reference』の「ACL commands」を参照してください。

- 3番目のカテゴリ: このルールは、認証されていないユーザーからのすべてのHTTP要求またはHTTPS要求をポータルWebサーバーにリダイレクトします。
- 4番目のカテゴリ: 直接認証の場合、ルールではユーザーパケットの通過が禁止されます。

ユーザーパケットを受信すると、デバイスは最初のカテゴリから4番目のカテゴリまでのフィルタリング規則とパケットを比較します。パケットが規則に一致すると、一致プロセスは完了します。

ポータルによるBYODのサポート

BYOD機能は、iMCサーバーと連動する必要があります。

ポータル認証中に、デバイスは取得したDHCPオプション55情報をポータルパケットおよびRADIUSパケットにカプセル化し、iMCサーバーのUAMコンポーネントにアップロードします。

DHCP Option55情報に基づいて、UAMはエンドポイントタイプ、OSおよびベンダー情報を識別します。UAMは様々な認証ページをプッシュし、様々な認可情報を様々なエンドポイントに配布します。

MACベースのクイックポータル認証

MACベースのクイックポータル認証は、ユーザーがネットワークに頻繁にアクセスするシナリオに適用されます。これにより、ユーザーはユーザー名とパスワードを入力せずに認証を渡すことができます。MACベースのクイックポータル認証は、MACトリガー認証または透過的ポータル認証とも呼ばれます。

MACトリガー認証には、MACバインディングサーバーが必要です。MACバインディングサーバーは、認証用のポータルユーザーのMACとアカウントのバインディングを記録します。アカウントには、ユーザー名およびパスワードを含むユーザーのポータル認証情報が含まれます。

MACベースのクイックポータル認証をサポートするのは、IPv4直接認証のみです。

認証は次のように実装されます。

1. ユーザーが初めてネットワークにアクセスする場合、アクセスデバイスは
   ユーザーのMACアドレスおよびアクセスインターフェイスを記録するMACトリガーエントリ。ユーザーのネットワークトラフィックがフリートラフィックのしきい値を下回る場合、ユーザーはポータル認証を実行せずにネットワークにアクセスできます。
2. ユーザーのネットワークトラフィックがしきい値に達すると、アクセスデバイスはMACバインディングクエリーをMACバインディングサーバーに送信します。
3. MACバインディングサーバーは、ユーザーのMACアドレスがポータルユーザーカウントにバインドされているかどうかをチェックします。
   - 一致するMACアカウントバインディングが存在する場合、MACバインディングサーバーはユ

ーザー認証情報をアクセスデバイスに送信してポータル認証を開始します。ユーザーはユーザー名とパスワードを入力せずに認証されます。

  - ユーザーがポータル認証に失敗した場合、認証失敗メッセージがユーザーに返されます。アクセスデバイス上のユーザーのMACトリガーエントリは、エントリが期限切れになると削除されます。
  - ユーザーがポータル認証を通過すると、アクセスデバイスはユーザーのMACトリガーエントリを削除します。

- 一致するMACアカウントバインディングが存在しない場合、MACバインディングサーバーは、ユーザーに対して通常のポータル認証を実行するようにアクセスデバイスに通知します。
  - ユーザーがポータル認証に失敗した場合、認証失敗メッセージがユーザーに戻されます。プロセス全体が終了します。
  - ユーザーがポータル認証を通過すると、アクセスデバイスはユーザーのMACアドレスと認証情報をMACバインディングサーバーに送信してMACアカウントバインディングを行います。さらに、アクセスデバイスはユーザーのMACトリガーエントリを削除します。

注:

- クライアントデータトラフィックを転送するようにAPが構成されているワイヤレスネットワークでは、APはトラフィック統計を定期的にACにレポートします。ACは、関連するAPからトラフィック統計レポートを受信した後にのみ、ユーザーのトラフィックが空きトラフィックのしきい値を超えているかどうかを判別できます。レポート間隔の設定の詳細は、「APがトラフィック統計をACにレポートする間隔の設定」を参照してください。
- MACバインディングサーバー設定の詳細については、サーバーのユーザーマニュアルを参照してください。

ワイヤレスネットワークでのポータル認証構成

FIT AP+ACネットワークのクライアントデータには、次の2つの転送モードがあります。

- 集中転送: APはクライアントからACにCAPWAPトンネルを介してデータフレームを送信し、ACはすべてのデータフレームを転送します。
- ローカル転送: APはクライアントからのデータフレームを、パケット転送のためにACに送信するのではなく、直接転送します。

ACでは、クライアントデータ転送モードに従って、VLANインターフェイスまたはサービステンプレート上でポータル認証を設定できます。

- VLANインターフェイス上のポータル認証は、集中型転送モードでのみ適用できます。

  ACは、VLANインターフェイスから受信したユーザーパケットだけを認証します。ローカル転送モードでは、ACはクライアントデータを受信できないため、クライアントに対してポータル認証を実行できません。
- サービステンプレートでのポータル認証は、集中型転送モードとローカル転送モードの両方で適用できます。

  ACは、集中型転送モードではこのAC上のBSSに、ローカル転送モードではAP上のBSSにポータルフィルタリング規則を導入します。ACは、サービステンプレートにバインドされているすべてのAPからユーザーを認証できます。

クライアントトラフィック転送の詳細については、『WLAN Access Configuration Guide』を参照してください。

ポータルユーザーのAC間ローミング

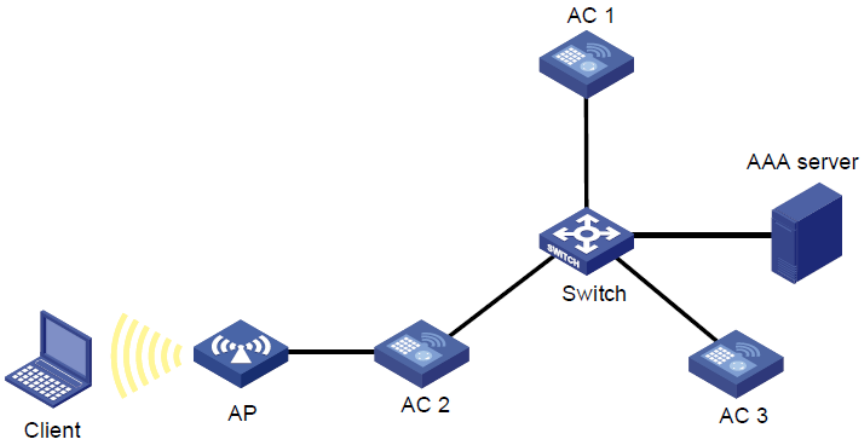
この機能により、ACで認証されたポータルユーザーは、別のACにローミングして、再認証なしでネットワークリソースにアクセスできます。

AC間ローミングでは、次のロールが関係します。

- WLANローミングセンターワイヤレスポータルユーザーの認証、承認、およびローミング情報を管理し、ユーザークエリサービスを提供します。
- ポータルローミングセンター認証およびローミングサービスを提供します。

図5に示すように、AC1はWLANローミングセンターとして機能し、AC2およびAC3はポータルローミングセンターとして機能します。

図5 ポータルユーザーのAC間ローミング



クライアントは最初にAC2でオンラインになり、AC3にローミングした後、次のようにオフラインになります。

1. クライアントはAC2でオンラインになります。
   a. クライアントがオンラインになることを要求すると、AC2はユーザークエリー要求をAC1に送信します。
   b. AC1はAC2にユーザークエリー応答を送信して、一致するポータルユーザーが見つからなかったことをAC2に通知します。
   c. AC2はクライアント上でポータル認証を実行します。
   d. クライアントがポータル認証にパスした後、AC2はユーザーオンラインパケットをAC1に送信し、クライアントがオンラインになったことをAC1に通知します。ユーザーオンラインパケットには、AAAサーバーがクライアントに割り当てる認可情報が含まれています。
   e. ユーザーオンラインパケットを受信すると、AC1はクライアントのユーザーエントリを作成し、ユーザーオンライン応答をAC2に送信します。ユーザーエントリには、クライアントのIPアドレス、MACアドレス、アクセスデバイスリスト、認可情報、およびローミング情報が含まれます。
2. クライアントはAC2からAC3にローミングします。
   a. クライアントがAC3でオンラインになることを要求すると、AC3はユーザークエリー要求をAC1に送信します。
   b. AC1はAC3に対してユーザー問合せ応答を送信し、一致するユーザーが見つかったことをAC3に通知します。ユーザー問合せ応答には、ユーザーがAC2を介してオンラインになったときに取得した認可情報が含まれます。
   c. ユーザークエリー応答を受信すると、AC3はクライアントが認証なしでオンラインになることを許可し、ユーザーオンラインパケットをAC1に送信します。

d. ユーザーオンラインパケットを受信すると、AC1はクライアントのユーザーエントリ内のローミング情報を更新し、ユーザーオンライン応答をAC3に送信する。

3. クライアントがオフラインになることを要求するか、クライアントがAC3によって強制的にログアウトされます。

- クライアントがオフラインになることを要求した場合、クライアントが最初にオンラインになるときに経由するAC(AC2)によってオフラインプロセスが開始されます。

  クライアントがオフラインになることを要求すると、AC2はユーザーを削除し、ユーザーオフラインパケットをAC1に送信します。ユーザーオフラインパケットを受信すると、AC1はユーザーエントリのアクセスデバイスリストからAC2を削除します。また、リスト内の他のアクセスデバイス(この例ではAC3)にもユーザーオフラインパケットを送信します。ユーザーオフラインパケットを受信すると、AC3はユーザーエントリを削除し、ユーザーオフラインレスポンスをAC1に送信します。

- クライアントがAC3によって強制的にログアウトされた場合、AC3はユーザーオフラインパケットをAC1に送信します。ユーザーオフラインパケットを受信すると、AC1はユーザーエントリのアクセスデバイスリストからAC3を削除し、ユーザーオフラインレスポンスをAC3に送信します。

ポータルユーザーが強制的にログアウトされる理由は、次のとおりです。

- 管理者は、アクセスデバイス上でコマンドを実行してユーザーをログアウトします。
- ユーザーがWLANにアクセスするために使用するAPがオフラインになります。
- ユーザーのDHCPリースが期限切れになります。
- ユーザーの認可アイドルタイムアウトタイマーまたは認可セッションタイムアウトタイマーが期限切れになります。
- 管理者はAAAサーバー上のユーザーをログアウトします。

制約事項およびガイドライン: ポータルの設定

デバイスは、許可ACL内のルールに一致するユーザートラフィックを、そのルールのpermitまたはdenyステートメントに基づいて処理します。ユーザートラフィックが許可ACLルールに一致しない場合、デバイスは異なるタイプのポータルユーザーに対して異なるアクションを実行します。

- 事前認証ユーザーの場合、デバイスは認証ページをプッシュしました。
- 認証されたユーザーの場合、デバイスはユーザーのすべてのパケットを許可します。

ポータルユーザーのトラフィックが認証ドメインの許可ACLのどのルールにも一致しない場合、デバイスはトラフィックを許可します。このようなトラフィックを拒否するには、rule deny ipコマンドを使用して、ACLの最後のルールを設定し、すべてのパケットを拒否します。

ポータルユーザーに割り当てられた許可ACLに、送信元IPv4、IPv6またはMACアドレスで指定されたルールがないことを確認します。ルールがない場合、ユーザーは認証を受けた後にオンラインにアクセスできません。許可ACLの詳細は、「AAAの構成」の許可属性の構成を参照してください。

デバイスは、HTTPS要求をポータルWebサーバーにリダイレクトしてポータル認証を行うことができます。SSL接続の確立中に、ユーザーブラウザに、サーバーIDを証明書で検証できないというメッセージが表示される場合があります。ユーザーがこのようなメッセージを確認せずにポータル認証を実行するには、SSLサーバーポリシーを構成して、クライアントが信頼できる証明書をデバイス上で要求します。ポリシーの名前はhttps_redirectである必要があります。SSLサーバーポリシーの構成の詳細は、「SSLの構成」を参照してください。証明書要求の詳細は、「PKIの構成」を参照してください。

Webを介したポータル認証では、ユーザーのセキュリティチェックはサポートされていません。セキュリ

ティチェックを実装するには、クライアントはH3C iNodeクライアントである必要があります。

ポータル認証は、WebクライアントまたはH3C iNodeクライアントによって開始されるNATトラバーサルをサポートします。NATトラバーサルは、ポータルクライアントがプライベートネットワークにあり、ポータルサーバーがパブリックネットワークにある場合に構成する必要があります。

ポータル認証タスクの概要

ポータル認証を設定するには、次のタスクを実行します。

1. リモートポータルサービスの構成

   リモートポータルサーバーを使用する場合は、次の作業を実行します。

   - リモートポータル認証サーバーの構成
   - ポータルWebサーバーの構成

2. ローカルポータルサービスの構成

   アクセスデバイスがポータル認証サーバーおよびポータルWebサーバーとして機能する場合は、次の作業を実行します。

   - ローカルポータルサービス機能の設定
   - ポータルWebサーバーの構成

3. ポータル認証の有効化とポータルWebサーバーの指定インターフェ

   イスまたはサービステンプレートで設定するオプションを選択します。

   - インターフェイスでのポータル認証のイネーブル化
   - インターフェイス上のポータルWebサーバーの指定
   - サービステンプレートでのポータル認証の有効化
   - サービステンプレートでのポータルWebサーバーの指定

4. (任意)事前認証ポータルユーザーのパラメータを設定します。

   - ポータル事前認証ドメインの構成
   - 事前認証IPアドレスプールの指定

5. (任意)ポータル認証ドメインの指定
6. (任意)ポータルユーザークセスの制御

   - ポータルフリールールの構成
   - 認証宛先サブネットの設定
   - ポータル禁止ルールの構成
   - デュアルスタックに対するポータル認証のサポートの設定
   - ポータルユーザーの最大数の設定
   - ポータル許可情報の厳密なチェックの有効化
   - DHCPによって割り当てられたIPアドレスを持つユーザーのみがポータル認証を通過できるようにする
   - 発信パケットフィルタリングのイネーブル化
   - ポータルユーザーのAC内ローミングを有効にする
   - ポータルフェール許可機能の設定
   - NAS-Port-Type属性の設定

- ワイヤレスクライアントでの有効性チェックの有効化

7. (任意)ポータル検出機能の設定
   - ポータルユーザーのオンライン検出の構成
   - ポータル認証サーバー検出の構成
   - ポータルWebサーバー検出の構成
   - ポータルユーザーの同期の構成
8. (任意)ポータルパケットおよびRADIUSパケットのアトリビュートの設定
   - ポータルパケット属性の設定

     ポータルパケットのBAS-IPまたはBAS-IPv6アトリビュートを設定し、デバイスIDを指定できます。
   - RADIUSパケットのアトリビュートの設定

     NAS-Port-Idアトリビュートフォーマットを設定し、NAS-IDプロファイルをインターフェイスに適用できます。
9. (任意)ユーザートラフィックバックアップしきい値の設定
10. (任意)MACベースのクイックポータル認証の設定
    a. リモートMACバインディングサーバーの設定
    b. ローカルMACバインディングサーバーの設定
    c. インターフェイス上のMACバインディングサーバーの指定
    d. サービステンプレートでのMACバインディングサーバーの指定
    e. クラウドMACトリガー認証を設定する
11. (任意)ポータルクライアントのルールARPまたはNDエントリ機能のディセーブル化
12. (任意)ポータルユーザーのトラフィックアカウンティングをディセーブルにします。
13. (任意)ポータルユーザー用のオンラインおよびオフライン関連機能の設定
    - ワイヤレスポータルユーザーを自動的にログアウトする
14. (任意)拡張ポータル認証機能の設定
    - Webリダイレクトの設定
    - ポータルセーフリダイレクトの設定
    - 単一ユーザーのポータルリダイレクトセッションの最大数の設定
    - APがトラフィック統計情報をACに報告する間隔の設定
    - ポータルプロトコルパケットからの属性の除外
    - サードパーティ認証用のポータル認証のサポートの構成
    - OAuthを使用したポータル認証のユーザー同期間隔の設定
    - ポータル認証情報レポートの間隔の構成
    - SS IDを切り替えるワイヤレスポータルユーザーのログアウト
    - ポータルオーセンティケータの中央ACへの切り替え
15. (任意)ポータル認証のモニタリング
    - ポータルロギングの有効化
    - ポータル認証監視機能の構成

ポータル認証の前提条件

ポータル機能は、ユーザーID認証およびセキュリティチェックのソリューションを提供します。ユーザーID認証を完了するには、ポータルがRADIUSと連携する必要があります。

ポータルを構成する前に、次のタスクを完了する必要があります。

- ポータル認証サーバー、ポータルWebサーバー、およびRADIUSサーバーが正しくインストールおよび構成されていること。
- ポータルクライアント、アクセスデバイス、およびサーバーは互いに接続できます。
- リモートRADIUSサーバーを使用するには、RADIUSサーバー上でユーザー名とパスワードを設定し、アクセスデバイス上でRADIUSクライアントを設定します。RADIUSクライアントの設定については、「AAAの設定」を参照してください。
- 拡張ポータル機能を実装するには、CAMS EADまたはiMC EADをインストールして設定します。アクセスデバイスに設定されているACLが、セキュリティポリシーサーバー上の隔離ACLおよびセキュリティACLに対応していることを確認します。アクセスデバイス上のセキュリティポリシーサーバー設定の詳細については、「AAAの設定」を参照してください。セキュリティポリシーサーバーのインストールおよび設定については、『CAMS EAD Security Policy Component User Manual』または『iMC EAD Security Policy Help』を参照してください。

リモートポータル認証サーバーの構成

このタスクについて

ポータル認証が有効になっている場合、デバイスは、受信したポータル要求パケットの送信元IPアドレス情報に従って、そのパケットのポータル認証サーバーを検索する。

- 一致するポータル認証サーバーが見つかった場合、デバイスはパケットを有効と見なし、認証応答パケットをポータル認証サーバーに送信します。ユーザーがデバイスにログインした後、ユーザーは必要に応じてポータル認証サーバーと対話します。
- 一致するポータル認証サーバーが見つからない場合、デバイスはパケットをドロップします。

制限事項およびガイドライン

使用中のポータル認証サーバーを削除しないでください。削除すると、そのサーバーによって認証されたユーザーは正しくログアウトできません。

手順

1. システムビューに入ります。

   system-view

2. ポータル認証サーバーを作成し、そのビューに入ります。

   portal server server-name

   複数のポータル認証サーバーを作成できます。

3. ポータル認証サーバーのIPアドレスを指定します。

   IPv4:

   ip ipv4-address [**key** { **cipher** | **simple** } *string*]

   IPv6:

   ipv6 ipv6-address [**key** { **cipher** | **simple** } *string*]

4. (任意)デバイスが非送信請求のポータルパケットをポータル認証サーバーに送信するために使用する宛先UDPポート番号を設定します。

   port port-number

   デフォルトでは、UDPポート番号は50100です。

   このポート番号は、ポータル認証サーバーで指定されたリスニングポート番号と同じである必要があります。

5. (任意)ポータル認証サーバータイプを指定します。

   server-type { cmcc | imc }

   デフォルトでは、ポータル認証サーバータイプはiMCです。

   指定するサーバータイプは、実際に使用されるポータル認証サーバーのタイプと同じである必要があります。

6. (任意)ログアウト通知パケットを再送信する最大回数と間隔を設定します。

   logout-notify retry retries interval *interval*

   デフォルトでは、デバイスはログアウト通知パケットを再送信しません。

7. (任意)定期的にポータル認証サーバーに登録するようにデバイスを設定します。

   server-register [**interval** *interval-value*]

デフォルトでは、デバイスはポータル認証サーバーに登録されません。

ポータルWebサーバーの構成

Portal Webサーバータスクの概要

ポータルWebサーバーを構成するには、次のタスクを実行します。

1. ポータルWebサーバーの基本パラメータを構成する
2. (任意)キャプティブバイパス機能のイネーブル化
3. (任意)URLリダイレクションの一致ルールの設定

ポータルWebサーバーの基本パラメータを構成する

1. システムビューに入ります。

   system-view
2. ポータルWebサーバーを作成し、そのビューに入ります。

   portal web-server server-name

   複数のポータルWebサーバーを作成できます。
3. ポータルWebサーバーのURLを指定します。

   url url-string

   デフォルトでは、ポータルWebサーバーのURLは指定されていません。
4. デバイスがURLをユーザーにリダイレクトするときにURLで伝送されるパラメータを設定します。

   url-parameter *param-name* { **nas-id** | **nas-port-id** | **original-url** | **source-address** | **ssid** | { **ap-mac** | **source-mac** } [**format section** { 1 | 3 | 6 } { **lowercase** | **uppercase** }] [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **value expression** | **vlan** }

   デフォルトでは、リダイレクションURLパラメータは設定されていません。
5. (任意)ポータルWebサーバーのタイプを指定します。

   Server-type {**cmcc | imc** | **oauth** | **wifidog**}

   デフォルトでは、ポータルWebサーバータイプはiMCです。

   この設定は、リモートポータルサービスだけに適用されます。

   指定するサーバータイプは、実際に使用されるポータルWebサーバーのタイプと同じである必要があります。

キャプティブバイパス機能のイネーブル化

このタスクについて

一般に、iOSモバイルデバイスまたは一部のAndroidモバイルデバイスがポータル対応ネットワークに接続されている場合、デバイスは認証ページをモバイルデバイスにプッシュします。

キャプティブバイパス機能を使用すると、ユーザーがブラウザを使用してインターネットにアクセスした場合にのみ、iOSおよびAndroidデバイスにポータル認証ページをプッシュできます。ユーザーが認証を実行せずにホームボタンを押してデスクトップに戻ると、Wi-Fi接続が終了します。このような場合に

Wi-Fi接続を維持するには、最適化されたキャプティブバイパス機能を有効にします。

Optimized Captive-Bypassがイネーブルの場合、ポータル認証ページは、iOSモバイルデバイスがネットワークに接続した後に自動的にiOSモバイルデバイスにプッシュされます。を実行するか、ホームボタンを押して認証を実行せずにデスクトップに戻ることができ、Wi-Fi接続は終了しません。

iOSクライアントがネットワークに接続されると、自動的にサーバー到達可能性検出パケットが送信され、Appleサーバーが到達可能かどうかが判断されます。サーバーが到達可能な場合は、Wi-Fi接続が接続されていると表示されます。サーバーが到達可能でない場合は、Wi-Fi接続が終了します。

ネットワーク状態が不良の場合、デバイスは、キャプティブバイパス検出タイムアウト時間内に、iOSモバイルクライアントからのサーバー到達可能性検出パケットを検出できません。クライアントは、サーバー到達可能性検出パケットに対する応答を受信できないため、サーバーが到達不能であると判断し、Wi-Fi接続を終了します。サーバー到達可能性検出障害によるWi-Fi切断を回避するには、ネットワーク状態が不良の場合に、キャプティブバイパス検出タイムアウト時間を長く設定してください。

手順

1. システムビューに入ります。

   system-view
2. ポータルWebサーバービューに入ります。

   portal web-server server-name
3. キャプティブパス機能をイネーブルにします。

   captive-bypass [android | ios [optimize]] enable

   デフォルトでは、キャプティブバイパス機能はディセーブルです。iOSモバイルデバイスおよび一部のAndroidモバイルデバイスがポータル対応ネットワークに接続されている場合、デバイスは自動的にポータル認証ページをこれらのデバイスにプッシュします。
4. (任意)キャプティブバイパス検出のタイムアウト時間を設定します。
   a. システムビューに戻ります。

      quit
   b. キャプティブバイパス検出のタイムアウト時間を設定します。

      portal captive-bypass optimize delay seconds

      デフォルトでは、キャプティブバイパス検出タイムアウト時間は6秒です。

URLリダイレクションの一致ルールの設定

このタスクについて

URLリダイレクション一致ルールは、ユーザーが要求したURLまたはユーザーエージェント情報によるHTTPまたはHTTPS要求を一致させ、一致するHTTPまたはHTTPS要求を指定されたリダイレクションURLにリダイレクトします。

ポータルWebサーバーの場合、URLリダイレクト用にurlコマンドおよびif-matchコマンドを構成できます。urlコマンドは、認証されていないユーザーからのすべてのHTTPまたはHTTPS要求をポータルWebサーバーにリダイレクトして認証を受けます。if-matchコマンドを使用すると、特定のHTTPまたはHTTPS要求を特定のリダイレクトURLにリダイレクトすることにより、柔軟なURLリダイレクトが可能になります。

制限事項およびガイドライン

ユーザーがリダイレクションURLに正常にアクセスできるようにするには、リダイレクションURL宛てのHTTP要求またはHTTPS要求の通過を許可するポータルフリー規則を設定します。ポータルフリー規

則の設定の詳細については、portal free-ruleコマンドを参照してください。

urlコマンドとif-matchコマンドの両方を実行した場合は、if-matchコマンドが優先されてURLリダイレクションが実行されます。

ポータルセーフリダイレクトおよびURLリダイレクションの両方の一致ルールが設定されている場合、デバイスは優先的にURLリダイレクション一致ルールを使用してURLリダイレクションを実行します。

手順

1. システムビューに入ります。

   system-view
2. ポータルWebサーバービューに入ります。

   portal web-server server-name
3. URLリダイレクションの一致ルールを設定します。

   if-match { **original-url** *url-string* **redirect-url** *url-string*
   [**url-param-encryption** { **aes | des** } **key { cipher | simple** } **string**] |
   user-agent *string* **redirect-url** *url-string* }

ローカルポータルサービス機能の設定

ローカルポータルサービスについて

ローカルポータルサービスの構成後、デバイスはポータルWebサーバーおよびポータル認証サーバーとして機能し、ユーザーに対してポータル認証を実行します。ポータル認証ページファイルは、デバイスのルートディレクトリに保存されます。

ローカルポータルサービス機能を設定するための制約事項およびガイドライン

インターフェイスがローカルポータルサービスを使用するには、インターフェイスに指定されたポータルWebサーバーのURLが次の要件を満たしている必要があります。

- URL内のIPアドレスは、デバイス上のレイヤ3インターフェイス(127.0.0.1を除く)のIPアドレスである必要があります。また、IPアドレスはポータルクライアントに到達可能である必要があります。
- URLは/portal/で終わる必要があります。例:http://1.1.1.1/portal/。

認証ページをカスタマイズして、デバイスにアップロードする必要があります。

http://1.1.1.1/portal/

ワイヤレスネットワークでは、異なるSSIDに属し、異なるデバイスタイプ(iPhoneやSamsungなど)を使用するポータルユーザーに対して、異なる認証ページをバインドできます。次の順序で認証ページが選択されます。

1. SSIDまたはデバイスタイプにバインドされた認証ページ。
2. デフォルトの認証ページ。

認証ページのカスタマイズ

このタスクについて

認証ページはHTMLファイルです。ローカルポータルの認証には、次の認証ページが必要です。

- ログオンページ
- ログオンの成功ページ
- ログオン失敗ページ
- オンラインページ
- システムビジーページ
- ログオフの成功ページ

認証ページをカスタマイズする必要があります。これには、認証ページで使用するページ要素も含まれます。たとえば、認証ページlogon.htmにはback.jpgが使用されます。

認証ページファイルを編集するときは、認証ページのカスタマイズ規則に従います。

ファイル名の規則

メイン認証ページファイルの名前は固定されています(表1を参照)。メイン認証ページファイル以外のファイルの名前を定義できます。ファイル名およびディレクトリ名の大文字と小文字は区別されません。

表1 主な認証ページファイル名

メイン認証ページ	ファイル名
ログオンページ	logon.htm
ログオンの成功ページ	logonSuccess.htm
ログオン失敗ページ	logonFail.htm
オンラインページ ユーザーがオンライン通知のためにオンラインになった後にプッシュされる	online.htm
システムビジーページ システムがビジーの場合、またはユーザーがログオンプロセス中の場合にプッシュされます。	busy.htm
ログオフの成功ページ	logoffSuccess.htm

ページ要求ルール

ローカルポータルのWebサービスは、Get要求とPost要求のみをサポートします。

- Get requests-認証ページ内の静的ファイルを取得し、再帰を許可しないために使用されます。たとえば、ファイルlogon.htmにファイルca.htmに対するGetアクションを実行するコンテンツが含まれている場合、ファイルca.htmにファイルlogon.htmへの参照を含めることはできません。
- 要求の転記ユーザーがユーザー名とパスワードのペアを送信し、ログインおよびログアウトするときに使用されます。

要求後の属性ルール

1. 認証ページのフォームを編集する場合は、次の要件に従ってください。
    - 認証ページには複数のフォームを含めることができますが、アクションがlogon.cgiであるフォームは1つだけである必要があります。そうでない場合、ユーザー情報をアクセスデバイスに送信できません。

- username属性はPtUserに固定されています。password属性はPtPwdに固定されています。
- PtButton属性の値はLogonまたはLogoffであり、ユーザーが要求するアクションを示します。
- ログオンPost要求には、PtUser、PtPwd、およびPtButton属性が含まれている必要があります。
- ログオフポスト要求には、PtButton属性が含まれている必要があります。

2. 認証ページlogon.htmおよびlogonFail.htmには、ログオンのPost要求が含まれている必要があります。次の例は、page logon.htmのスクリプトの一部を示しています。

```
<form action=logon.cgi method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px" maxlength=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px" maxlength=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;">
</form>
```

3. 認証ページlogonSuccess.htmおよびonline.htmには、ログオフのPost要求が含まれている必要があります。

次の例は、page online.htm内のスクリプトの一部を示しています。

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

ページファイルの圧縮と保存の規則

認証ページとそのページ要素を標準のzipファイルに圧縮する必要があります。

- zipファイルの名前には、文字、数字、および下線のみを使用できます。
- 認証ページは、zipファイルのルートディレクトリに配置する必要があります。
- ZIPファイルはFTPまたはTFTPを介してデバイスに転送でき、デバイスのルートディレクトリに保存する必要があります。

デバイス上のzipファイルの例:

```
<Sysname> dir
Directory of flash:
   1     -rw-      1405   Feb  28  2008  15:53:20       ssid1.zip
   0     -rw-      1405   Feb  28  2008  15:53:31       ssid2.zip
   2     -rw-      1405   Feb  28  2008  15:53:39       ssid3.zip
   3     -rw-      1405   Feb  28  2008  15:53:44       ssid4.zip
2540 KB total (1319 KB free)
```

認証されたユーザーを特定のWebページにリダイレクトする

デバイスが認証済みユーザーを特定のWebページに自動的にリダイレクトするようにするには、logon.htmおよびlogonSuccess.htmで次の手順を実行します。

1. logon.htmで、Formのtarget属性を_blankに設定します。内容は灰色で表示されます。

```
<form method=post action=logon.cgi target="_blank">
```

2. pt_init()を読み込むページの関数をLogonSuccess.htmに追加します。

内容を灰色で表示する:

```
<html>
<head>
```

```
        <title>LogonSuccess</title>
            <script type="text/javascript" language="javascript"
            src="pt_private.js"></script>
        </head>
        <body onload="pt_init();" onbeforeunload="return pt_unload();">
        ... ...
        </body>
</html>
```

ローカルポータルWebサービスの構成

前提条件

HTTPSベースのローカルポータルWebサービスを構成する前に、次のタスクを完了する必要があります。

- PKIポリシーを構成し、CA証明書を取得し、ローカル証明書を要求します。詳細は、「PKIの構成」を参照してください。
- SSLサーバーポリシーを設定し、PKIポリシーで設定されたPKIドメインを指定します。

  SSL接続の確立中に、ユーザーブラウザに、サーバーIDを証明書で検証できないというメッセージが表示される場合があります。ユーザーがこのようなメッセージを確認せずにポータル認証を実行するには、SSLサーバーポリシーを構成して、クライアントで信頼できる証明書をデバイスに要求します。ポリシーの名前はhttps_redirectである必要があります。SSLサーバーポリシーの構成の詳細は、「SSLの構成」を参照してください。
- ポータル認証前にローカルポータルへredirectするためにDNSへアクセスする必要がありますが、DNSのサイトを指定するよりは、汎用的なDNSのポート番号でアクセスを許可します。

  portal free-rule 1 destination ip any udp 53

  portal free-rule 2 destination ip any tcp 53

  「ポータルユーザーアクセスの制御」参照
- (任意)client forwarding-location ap(ユーザーデータをCAPWAPトンネルを通さずに、直接VLAN内を通す設定)の場合、以下のコマンドが必要。

  [AC] portal host-check enable

手順

1. システムビューに入ります。

   system-view
2. HTTPまたはHTTPSベースのローカルポータルWebサービスを作成し、そのビューに入ります。

   portal local-web-server { http | https [ssl-server-policy *policy-name*] [**tcp-port** *port-number*] }
3. ローカルポータルWebサービスの既定の認証ページファイルを指定します。

   default-logon-page filename

   既定では、ローカルポータルWebサービスに既定の認証ページファイルは指定されていません。
4. (任意)ローカルポータルWebサービスのリスニングTCPポートを設定します。

   tcp-port port-number

   デフォルトでは、HTTPサービスリスニングポート番号は80で、HTTPSサービスリスニングポート番号は、portal local-web-serverコマンドによって設定されたTCPポート番号です。

5. (任意)SSIDまたはエンドポイントタイプを認証ページファイルにバインドします。

   logon-page bind { device-type { computer | pad | phone } | device-name *device-name* | **ssid** *ssid-name* } * *file file-name*

   デフォルトでは、SSIDまたはエンドポイントタイプは認証ページファイルにバインドされません。

   例

   # HTTPベースのローカルポータルWebサービスを作成します。

   <Sysname> **system-view**

   [Sysname] **portal local-web-server http**

   # SSID **SSID1**を認証ページファイル**file1.zip**にバインドします。

   [Sysname-portal-local-websvr-http] **logon-page bind ssid SSID1 file file1.zip**

   # エンドポイントタイプのcomputerを認証ページファイルfile2.zipにバインドします。

   [Sysname-portal-local-websvr-http] **logon-page bind device-type computer file file2.zip**

6. (任意)ローカルポータルユーザーパスワードの変更をイネーブルにします。

   user-password modify enable

   デフォルトでは、ローカルポータルユーザーパスワードの変更は無効です。

User-Agent一致文字列の設定

このタスクについて

ポータルユーザーがサードパーティソフトウェアを使用してポータル認証を実行する場合、デバイスはポータル認証要求のUser-Agent文字列をチェックします。User-Agent文字列にデバイスで指定された一致文字列が含まれていない場合、ユーザーはポータル認証に失敗します。

User-Agent文字列には、ハードウェアベンダー、ソフトウェアオペレーティングシステム、ブラウザおよび検索エンジンの情報が含まれます。次のタスクを実行して、サードパーティソフトウェアのUser-Agent情報と一致する文字列を指定します。これにより、ユーザーは、そのサードパーティソフトウェアを使用してポータル認証を渡すことができます。たとえば、ユーザーがWeChatの公式アカウントに従ってポータル認証を渡す場合は、デバイス上のUser-Agent一致文字列をMicroMessengerとして構成します。

手順

1. システムビューに入ります。

   system-view

2. ローカルポータルのWebサービスビューに入ります。

   portal local-web-server { http | https [ssl-server-policy *policy-name*] [**tcp-port** *port-number*] }

3. User-Agent一致文字列を設定します。

   user-agent user-agent-string

   デフォルトでは、User-Agentの一致文字列はMicroMessengerです。

インターフェイスでのポータル認証のイネーブル化

制限事項およびガイドライン

インターフェイスでポータル認証をイネーブルにする場合は、次の制約事項および注意事項に従ってくだ

さい。

- インターフェイスとサービステンプレートの両方でポータル認証をイネーブルにしないでください。
- インターフェイス上でIPv4ポータル認証とIPv6ポータル認証の両方をイネーブルにできます。

手順

1. システムビューに入ります。
   system-view
2. レイヤー3 interfaceビューに入ります。
   interface interface-type interface-number
3. ポータル認証を有効にしま
   す。IPv4:
   portal enable method direct
   IPv6:
   portal ipv6 enable method direct
   デフォルトでは、ポータル認証はディセーブルです。

インターフェイス上のポータルWebサーバーの指定

このタスクについて

インターフェイス上でポータルWebサーバーを指定すると、デバイスはインターフェイス上のポータルユーザーのHTTP要求をポータルWebサーバーにリダイレクトします。

インターフェイスには、IPv4ポータルWebサーバーとIPv6ポータルWebサーバーの両方を指定できます。

手順

1. システムビューに入ります。
   system-view
2. レイヤー3 interfaceビューに入ります。
   interface interface-type interface-number
3. インターフェイス上のポータルWebサーバーを指定します。
   portal [**ipv6**] **apply web-server** *server-name* [**secondary**]
   デフォルトでは、インターフェイスにポータルWebサーバーは指定されません。

サービステンプレートでのポータル認証の有効化

制限事項およびガイドライン

インターフェイスとサービステンプレートの両方でポータル認証を有効にしないでください。サービステン

プレートでは、直接ポータル認証のみがサポートされます。

ワイヤレスネットワークでローカル転送を使用する場合は、ワイヤレスクライアントの有効性チェックを有効にします。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template service-template-name
3. サービステンプレートで直接ポータル認証をイネーブルにします。
   portal [ipv6] enable method direct
   デフォルトでは、直接ポータル認証はサービステンプレートで無効になっています。

サービステンプレートでのポータルWebサーバーの指定

このタスクについて

ポータルWebサーバーが指定されている場合、デバイスは、指定されたサービステンプレートにバインドされwlan-BSSインターフェイス上のポータルユーザーからのHTTP要求を、指定されたポータルWebサーバーにリダイレクトします。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template service-template-name
3. サービステンプレートにポータルWebサーバーを指定します。
   portal [**ipv6**] **apply web-server** *server-name* [**secondary**]
   デフォルトでは、サービステンプレートにポータルWebサーバーは指定されていません。

ポータル事前認証ドメインの構成

このタスクについて

ポータル事前認証ドメインは、ユーザーがIPアドレスを取得した後に、ポータル対応のインターフェイスで事前認証ポータルユーザーに割り当てられたユーザー属性を定義します。事前認証ユーザーは、ポータル認証を通過する前に、割り当てられたユーザー属性(ACL、ユーザープロファイル、CARなど)に基づいてネットワークへのアクセスが制限されます。ユーザーがポータル認証を通過すると、AAAサーバーによって新しい属性が割り当てられます。ユーザーがオフラインになると、事前認証ドメイン内でユーザー属性が再割り当てされます。

制限事項およびガイドライン

ポータル事前認証ドメインは、DHCPまたはDHCPv6を介して取得されたIPアドレスを持つポータルユーザーに対してのみ有効です。

ポータル事前認証ドメインは、クロスサブネットポータル認証がイネーブルになっているインターフェイスでは有効になりません。

既存のISPドメインをポータル事前認証ドメインとして指定していることを確認してください。指定されたISPドメインが存在しない場合、デバイスが正しく動作しない可能性があります。

次の状況では、事前認証ドメインを削除し(undo portal[ipv6]pre-auth domainコマンドを使用)、再構成する必要があります。

- ISPドメインは、事前認証ドメインとして指定した後に作成します。
- 指定したISPドメインを削除してから、再作成します。

事前認証ドメイン内の許可ACLには、次の規則が適用されます。

- ACLが存在しない場合、またはACL内のルールによって許可された宛先アドレスがanyに設定されている場合、デバイスはユーザーアクセスを制御しません。ユーザーは、ポータル認証を受けずに任意のネットワークリソースにアクセスできます。
- ACLにルールが設定されていない場合は、ユーザーが認証にパスした後にだけ、デバイスによってネットワークリソースへのアクセスが許可されます。
- ソースアドレスは指定しないでください。ソースアドレスを指定すると、ユーザーはポータル認証をトリガーできません。

事前認証ドメインとMACトリガー認証の両方がデバイスに設定されている場合は、MACトリガー認証の空きトラフィックしきい値を0バイトに設定します。

手順

1. システムビューに入ります。

   system-view
2. interface viewに入ります。

   interface interface-type interface-number
3. ポータル事前認証ドメインを指定します。

   portal [**ipv6**] **pre-auth domain** *domain-name*

   デフォルトでは、ポータル事前認証ドメインは指定されていません。

事前認証IPアドレスプールの指定

このタスクについて

次の状況では、ポータル対応インターフェイス上で事前認証IPアドレスプールを指定する必要があります。

- ポータルユーザーは、ポータル対応インターフェイスのサブインターフェイスを介してネットワークにアクセスします。
- サブインターフェイスにはIPアドレスがありません。
- ポータルユーザーは、DHCPを使用してIPアドレスを取得する必要があります。

ユーザーがポータル対応のインターフェイスに接続した後、ユーザーは次の規則に従ってポータル認証にIPアドレスを使用します。

- インターフェイスに事前認証IPアドレスプールが設定されている場合、ユーザーは次のIPアドレスを使用します。
  - クライアントがDHCPを介して自動的にIPアドレスを取得するように設定されている場合、ユーザーは指定されたIPアドレスプールからアドレスを取得します。
  - クライアントが静的IPアドレスで構成されている場合、ユーザーは静的IPアドレスを使用します。ただし、インターフェイスにIPアドレスがない場合、静的IPアドレスを使用するユーザーは認証を通過できません。

- インターフェイスにIPアドレスが設定されているが、事前認証IPプールが指定されていない場合、ユーザーはスタティックIPアドレスまたはDHCPサーバーから取得したIPアドレスを使用します。
- インターフェイスにIPアドレスまたは事前認証IPプールが指定されていない場合、ユーザーはポータル認証を実行できません。

ユーザーがポータル認証を通過した後、AAAサーバーはユーザーにIPアドレスを再割り当てするためにIPアドレスプールを認可します。認可されたIPアドレスプールが展開されていない場合、ユーザーは以前のIPアドレスを引き続き使用します。

制限事項およびガイドライン

この設定は、直接IPv4ポータル認証がインターフェイス上でイネーブルになっている場合にだけ有効になります。

指定されたIPアドレスプールが存在し、完全であることを確認してください。それ以外の場合、ユーザーはIPアドレスを取得できず、ポータル認証を実行できません。

ポータルユーザーが認証を実行しないか、認証に失敗した場合でも、割り当てられたIPアドレスは保持されます。

手順

1. システムビューに入ります。
   system-view
2. レイヤー3 interfaceビューに入ります。
   interface interface-type interface-number
3. インターフェイス上で事前認証IPアドレスプールを指定します。
   portal [**ipv6**] **pre-auth ip-pool** *pool-name*
   デフォルトでは、事前認証IPアドレスプールはインターフェイス上で指定されません。

ポータル認証ドメインの指定

ポータル認証ドメインについて

認証ドメインは、一連の認証、認可および会計ポリシーを定義します。各ポータルユーザーは認証ドメインに属し、ドメインで認証、認可および会計処理されます。

インターフェイスまたはサービステンプレートで指定された認証ドメインにより、デバイスはポータルユーザーのAAAに対して認証ドメインを使用します。これにより、柔軟なポータルアクセスコントロールが可能になります。

ポータル認証ドメインを指定するための制限事項とガイドライン

デバイスは、次の順序でポータルユーザーの認証ドメインを選択します。

1. インターフェイスまたはサービステンプレートに指定されたISPドメイン。
2. ユーザー名で伝送されるISPドメイン。
3. システムのデフォルトISPドメイン。

選択したドメインがデバイスに存在しない場合、デバイスは、存在しないドメインに割り当てられたユー

ザーを受け入れるように構成されたISPドメインを検索します。このようなISPドメインが構成されていない場合、ユーザー認証は失敗します。ISPドメインの詳細は、「AAAの構成」を参照してください。

インターフェイス上のポータル認証ドメインの指定

1. システムビューに入ります。
   system-view
2. レイヤー3 interfaceビューに入ります。
   interface interface-type interface-number
3. インターフェイス上のポータル認証ドメインを指定します。
   portal [ipv6] domain *domain-name*
   デフォルトでは、インターフェイスにポータル認証ドメインは指定されていません。
   インターフェイスには、IPv4ポータル認証ドメインとIPv6ポータル認証ドメインの両方を指定できます。

サービステンプレートでのIPv4ポータル認証ドメインの指定

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template service-template-name
3. サービステンプレートにポータル認証ドメインを指定します。
   portal [**ipv6**] **domain** *domain-name*
   デフォルトでは、サービステンプレートにポータル認証ドメインは指定されていません。

ポータルユーザーアクセスの制御

ポータルフリールールの構成

このタスクについて

ポータルフリー規則を使用すると、指定したユーザーは、ポータル認証なしで指定した外部Webサイトにアクセスできます。

ポータルフリー規則の一致項目には、ホスト名、送信元/宛先IPアドレス、TCP/UDPポート番号、送信元MACアドレス、アクセスインターフェイス、およびVLANが含まれます。ポータルフリー規則に一致するパケットはポータル認証をトリガーしないため、パケットを送信するユーザーは指定された外部Webサイトに直接アクセスできます。

ポータルフリールールの構成に関する制約事項およびガイドライン

VLANとインターフェイスの両方を指定する場合、インターフェイスはVLANに属している必要があります。インターフェイスがVLANに属していない場合、ポータルフリー規則は有効になりません。

同じフィルタ条件を使用して2つ以上のポータルフリールールを構成することはできません。それ以外の場合は、ルールがすでに存在することを示すプロンプトが表示されます。

ポータル認証が有効になっているかどうかにかかわらず、ポータルフリールールは追加または削除のみ可能です。変更はできません。

ソースベースのポータルフリー規則が設定される前にポータルユーザーがオンラインになった場合、デバイスはユーザーのトラフィックに対してアカウンティングを実行し続けます。

IPベースのポータルフリー規則の設定

1. システムビューに入ります。

   system-view

2. IPベースのポータルフリー規則を設定します。

   IPv4:

   portal free-rule *rule-number* **{ destination ip { ipv4-address** { *mask-length* | **mask** } | **any** } [tcp *tcp-port-numbe*r | **udp** *udp-port-numbe*r] | **source ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

   IPv6:

   portal free-rule *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-numbe*r | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [i**nterface** *interface-type interface-number*]

   デフォルトでは、IPベースのポータルフリー規則は設定されていません。

ソースベースのポータルフリールールの構成

1. システムビューに入ります。

   system-view

2. ソースベースのポータルフリー規則を設定します。

   portal free-rule *rule-number* **source** { **ap** *ap-name* | { **interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } * }

   デフォルトでは、ソースベースのポータルフリー規則は設定されていません。

   vlan vlan-idオプションは、VLANインターフェイスを介してネットワークにアクセスするポータルユーザーに対してだけ有効です。

宛先ベースのポータルフリールールの構成

1. システムビューに入ります。

   system-view

2. 宛先ベースのポータルフリー規則を設定します。

   portal free-rule rule-number destination host-name

   デフォルトでは、宛先ベースのポータルフリー規則は設定されていません。

ポータルフリールールの説明の構成

1. システムビューに入ります。

   system-view

2. ポータルフリー規則の説明を設定します。

   portal free-rule rule-number description text

   デフォルトでは、ポータルフリールールの説明は構成されません。

認証宛先サブネットの設定

このタスクについて

認証宛先サブネットを構成することにより、ユーザーが指定されたサブネット(ポータルフリールールで指定された宛先IPアドレスおよびサブネットを除く)にアクセスする場合にのみポータル認証をトリガーするように指定します。ユーザーは、ポータル認証なしで他のサブネットにアクセスできます。

制限事項およびガイドライン

複数の認証宛先サブネットを設定できます。宛先サブネットが重複する場合は、最大のアドレス範囲(最小のマスクまたはプレフィクス)を持つサブネットが有効になります。

手順

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. ポータル認証の宛先サブネットを構成します。

   IPv4:

   portal free-all except destination *ipv4-network-address* { *mask-length* | *mask* }

   IPv6:

   portal ipv6 free-all except destination *ipv6-network-address prefix-length*

   デフォルトでは、サブネットにアクセスするユーザーはポータル認証をパスする必要があります。

ポータル禁止ルールの構成

このタスクについて

ポータル禁止規則は、指定された送信元からのユーザーパケットまたは指定された宛先宛てのユーザーパケットをフィルタリングするために使用されます。デバイスは、ポータル禁止規則に一致するHTTPまたはHTTPSパケットをドロップします。

制限事項およびガイドライン

ポータル禁止規則では、送信元と宛先のIPアドレスは同じIPタイプでなければならず、送信元と宛先のポートは同じトランスポートプロトコルタイプでなければなりません。

複数のポータル禁止規則を設定できます。

ポータルフリー規則とポータル禁止規則のソース情報または宛先情報が重複する場合、ポータル禁止規則が有効になります。

ポータル禁止ルールで宛先ホスト名を指定すると、デバイスは指定されたホスト名に対するユーザーのDNS問合せパケットをドロップします。さらに、DNSサーバーがデバイス上で正しく構成されている場合、デバイスは指定されたホスト名から解決されたIPアドレス宛てのユーザーパケットもドロップします。DNSサーバーが正しく構成されていない場合、ルールはそのIPアドレス宛てのユーザーパケットには影響しません。

手順

1. システムビューに入ります。

   system-view

2. ポータル禁止規則を設定します。

   IPv4:

   portal forbidden-rule *rule-number* [**source** { **ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **ssid** *ssid-name* } *] **destination** { *host-name* | **ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] }

   IPv6:

   portal forbidden-rule *rule-numbe*r [**source** { **ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-numbe*r | **udp** *udp-port-number*] | **ssid** *ssid-name* } *] **destination** { *host-name* | **ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] }

   デフォルトでは、ポータル禁止規則が設定されています。

デュアルスタックに対するポータル認証のサポートの設定

このタスクについて

通常、IPv4ポータルユーザーはポータル認証を通過した後にIPv4ネットワークにのみアクセスでき、IPv6ポータルユーザーはポータル認証を通過した後にIPv6ネットワークにのみアクセスできます。ポータルユーザーが1つのタイプ(IPv4またはIPv6)のポータル認証を通過した後にIPv4とIPv6の両方のネットワークにアクセスできるようにするには、ポータルのデュアルスタック機能を有効にします。

インターフェイス上のデュアルスタックに対するポータル認証のサポートの設定

1. システムビューに入ります。

   system-view

2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number

3. インターフェイス上でポータルデュアルスタック機能をイネーブルにします。

   portal dual-stack enable

   デフォルトでは、ポータルデュアルスタック機能はインターフェイス上でディセーブルです。

4. インターフェイス上のデュアルスタックポータルユーザーに対して、個別のIPv4およびIPv6トラフィック統計情報をイネーブルにします。

   portal dual-stack traffic-separate enable

   デフォルトでは、インターフェイス上のデュアルスタックポータルユーザーに対して個別のIPv4およびIPv6トラフィック統計情報はディセーブルです。デバイスは、IPv4およびIPv6トラフィック統計情報をまとめて収集します。

5. デュアルIP機能をイネーブルにして、リモートポータル認証でシングルスタックユーザーのIPv4アドレスとIPv6アドレスの両方を伝送できるようにします。

   portal dual-ip enable

   デフォルトでは、デュアルIP機能はディセーブルです。

6. ポータルユーザーのオフラインログで個別のIPv4およびIPv6トラフィック統計情報を有効にします。

   portal user-log traffic-separate

   デフォルトでは、ポータルユーザーのIPv4およびIPv6トラフィック統計は、ポータルユーザーのオフラ

インログ内でIPv4トラフィック統計としてまとめてカウントされます。

サービステンプレート上のデュアルスタックに対するポータル認証のサポートの設定

1. システムビューに入ります。

   system-view

2. サービステンプレートビューに入ります。

   wlan service-template service-template-name

3. サービステンプレートでポータルデュアルスタック機能をイネーブルにします。

   portal dual-stack enable

   デフォルトでは、サービステンプレート上のポータルデュアルスタック機能はディセーブルです。

4. サービステンプレート上のデュアルスタックポータルユーザーに対して、個別のIPv4およびIPv6トラフィック統計情報をイネーブルにします。

   portal dual-stack traffic-separate enable

   デフォルトでは、サービステンプレート上のデュアルスタックポータルユーザーに対して、個別のIPv4およびIPv6トラフィック統計情報はディセーブルです。デバイスは、IPv4およびIPv6トラフィック統計情報をまとめて収集します。

5. デュアルIP機能をイネーブルにして、リモートポータル認証でシングルスタックユーザーのIPv4アドレスとIPv6アドレスの両方を伝送できるようにします。

   portal dual-ip enable

   デフォルトでは、デュアルIP機能はディセーブルです。

6. ポータルユーザーのオフラインログで個別のIPv4およびIPv6トラフィック統計情報を有効にします。

   portal user-log traffic-separate

   デフォルトでは、ポータルユーザーのIPv4およびIPv6トラフィック統計は、ポータルユーザーのオフラインログ内でIPv4トラフィック統計としてまとめてカウントされます。

ポータルユーザーの最大数の設定

このタスクについて

システム内のポータルユーザーの総数と、インターフェイスまたはサービステンプレート上のIPv4またはIPv6ポータルユーザーの最大数を制御するには、次の作業を実行します。

ポータルユーザーの最大数を設定するための制限およびガイドライン

すべてのインターフェイスまたはサービステンプレートで指定されたIPv4およびIPv6ポータルユーザーの最大合計数が、システムで許可されている最大数を超えていないことを確認してください。超えているポータルユーザー数は、デバイスにログインできません。

ポータルユーザーのグローバルな最大数の設定

1. システムビューに入ります。

   system-view

2. ポータルユーザーのグローバル最大数を設定します。

   portal max-user max-number

   デフォルトでは、ポータルユーザーのグローバル数に制限は設定されていません。

   グローバル最大数をデバイス上の現在のオンラインポータルユーザー数よりも小さく設定した場合でも、この構成は有効です。オンラインユーザーは影響を受けませんが、新規ポータルユーザ

ーのログインは禁止されます。

インターフェイス上のポータルユーザーの最大数の設定

1. システムビューに入ります。

   system-view

2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number

3. ポータルユーザーの最大数を設定します。

   portal { ipv4-max-user | ipv6-max-user } *max-number*

   デフォルトでは、インターフェイス上のポータルユーザー数に制限は設定されません。

   インターフェイス上のポータルユーザーの現在の数よりも小さい最大数を設定した場合でも、この設定は有効になります。オンラインユーザーは影響を受けませんが、新しいポータルユーザーがインターフェイスからログインすることはできません。

サービステンプレート上のポータルユーザーの最大数の設定

1. システムビューに入ります。

   system-view

2. サービステンプレートビューに入ります。

   wlan service-template service-template-name

3. ポータルユーザーの最大数を設定します。

   portal { ipv4-max-user | **ipv6-max-user** } *max-number*

   デフォルトでは、ポータルユーザー数に制限は設定されていません。

   サービステンプレート上のポータルユーザーの現在の数よりも小さい最大数を設定した場合でも、この構成は有効になります。オンラインユーザーは影響を受けませんが、新規ポータルユーザーはサービステンプレートからログインできません。

ポータル許可情報の厳密なチェックの有効化

このタスクについて

厳密チェック機能を使用すると、ポータルユーザーは、ユーザーの認可情報が正常に展開された場合に限り、オンライン状態を維持できます。厳密チェックは、認可されたACLまたはユーザープロファイルがデバイスに存在しない場合、またはデバイスが認可されたACLまたはユーザープロファイルの展開に失敗した場合に失敗します。

認可ACL、認可ユーザープロファイル、またはその両方に対して厳密なチェックを有効にできます。ACLチェックとユーザープロファイルチェックの両方を有効にした場合、どちらかのチェックに失敗するとユーザーはログアウトされます。

インターフェイス上のポータル認証情報に対する厳密なチェックの有効化

1. システムビューに入ります。

   system-view

2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number

3. ポータル許可情報の厳密なチェックをイネーブルにします。

   portal authorization { acl | user-profile } strict-checking

デフォルトでは、ポータル許可情報の厳密なチェックはインターフェイス上でディセーブルになっています。許可されたACLまたはユーザープロファイルが存在しない場合や、デバイスが許可されたACLまたはユーザープロファイルの展開に失敗した場合でも、ポータルユーザーはオンラインのままです。

サービステンプレート上のポータル許可情報に対する厳密なチェックの有効化

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. ポータル許可情報の厳密なチェックをイネーブルにします。

   portal authorization { acl | user-profile } strict-checking

   デフォルトでは、ポータル許可情報の厳密なチェックはサービステンプレートでは無効になっています。許可されたACLまたはユーザープロファイルが存在しない場合や、デバイスが許可されたACLまたはユーザープロファイルの配布に失敗した場合でも、ポータルユーザーはオンラインのままです。

DHCPによって割り当てられたIPアドレスを持つユーザーのみがポータル認証を通過できるようにする

このタスクについて

この機能を使用すると、DHCPによって割り当てられたIPアドレスを持つユーザーのみがポータル認証を通過できます。静的IPアドレスを持つユーザーは、ポータル認証を通過してオンラインになることはできません。有効なIPアドレスを持つユーザーのみがネットワークにアクセスできるようにするには、この機能を使用します。

制限事項およびガイドライン

この機能は、デバイスがアクセスデバイスとDHCPサーバーの両方として機能する場合にのみ有効になります。AC+fit APネットワークでは、この機能はACがDHCPサーバーとして機能する場合にのみ有効です。

この機能が構成されている場合、IPv6ユーザーがポータル認証を通過できるようにするには、端末デバイスで一時IPv6アドレス機能を無効にします。無効にしないと、IPv6ユーザーは一時IPv6アドレスを使用してIPv6ネットワークにアクセスし、ポータル認証に失敗します。

この機能の設定は、オンラインポータルユーザーには影響しません。

DHCPによって割り当てられたIPアドレスを持つユーザーのみが、インターフェイス上でポータル認証を通過できるようにする

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. DHC Pによって割り当てられたIPアドレスを持つユーザーだけにポータル認証の通過を許可します。

   portal [ipv6] user-dhcp-only

   デフォルトでは、DHCPを介して取得されたIPアドレスを持つユーザーと静的IPアドレスを持つユー

ザーの両方が、認証を通過してオンラインになることができます。

DHCPによって割り当てられたIPアドレスを持つユーザーのみが、サービステンプレートでポータル認証を通過できるようにする

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. DHCPによって割り当てられたIPアドレスを持つユーザーだけにポータル認証の通過を許可します。

   portal user-dhcp-only

   デフォルトでは、DHCPを介して取得されたIPアドレスを持つユーザーと静的IPアドレスを持つユーザーの両方が、認証を通過してオンラインになることができます。

発信パケットフィルタリングのイネーブル化

このタスクについて

ポータル対応のインターフェイスまたはサービステンプレートでこの機能をイネーブルにすると、デバイスはインターフェイスが次のパケットを送信することを許可します。

- 宛先IPアドレスが認証済みポータルユーザーのIPアドレスであるパケット。
- ポータルフリー規則に一致するパケット。

インターフェイスまたはサービステンプレート上のその他の発信パケットはドロップされます。

インターフェイスでの発信パケットフィルタリングのイネーブル化

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. インターフェイス上で発信パケットフィルタリングをイネーブルにします。

   portal [ipv6] outbound-filter enable

   デフォルトでは、発信パケットフィルタリングはインターフェイス上でディセーブルです。インターフェイスは任意のパケットを送信できます。

サービステンプレートでの発信パケットフィルタリングのイネーブル化

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. サービステンプレートで発信パケットフィルタリングをイネーブルにします。

   portal [ipv6] outbound-filter enable

   デフォルトでは、サービステンプレートでの発信パケットフィルタリングはディセーブルです。サービステンプレートは任意のパケットを送信できます。

ポータルユーザーのAC内ローミングを有効にする

このタスクについて

ポータルユーザーのAC内ローミングがVLANインターフェイスでイネーブルになっている場合、オンラインポータルユーザーは、再認証なしでVLAN内の任意のレイヤ2ポートからリソースにアクセスできます。

ポータルユーザーのAC内ローミングがディセーブルの場合、VLAN内の現在のアクセスポートとは異なるレイヤ2ポートから外部ネットワークリソースにアクセスするには、ユーザーは次の手順を実行する必要があります。

1. 現在のポートからログアウトします。
2. 新しいレイヤ2ポート上で再認証します。

制限事項およびガイドライン

オンラインポータルユーザーまたは事前認証ポータルユーザーがデバイス上に存在する場合は、AC内ローミングをイネーブルにできません。

AC内ローミングを有効にするには、ルールARPまたはNDエントリ機能をディセーブルにする必要があります。
undo portal refresh{arp nd}enableコマンド。

手順

1. システムビューに入ります。

   system-view
2. ポータルユーザーのAC内ローミングを有効にします。

   portal roaming enable

   デフォルトでは、ポータルユーザーのAC内ローミングは無効になっています。

ポータルユーザーのAC間ローミングの設定

このタスクについて

この機能を使用すると、ACで認証されたポータルユーザーは、別のACにローミングして、再認証なしにネットワークリソースにアクセスできます。この機能は、WLANローミングセンターと連携する必要があります。WLANローミングセンターの詳細については、『WLAN Roaming Configuration Guide』を参照してください。

ハードウェアと機能の互換性

ハードウェアシリーズ	モデル	製品コード	AC間ローミングの互換性
WX1800Hシリーズ	WX1804H	EWP-WX1804H-PWR-CN	いいえ
WX2500Hシリーズ	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	いいえ
	WX3010H WX3010H-X	EWP-WX3010H EWP-WX3010H-X-PWR	

WX3000Hシリーズ	WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	いいえ
WX3500Hシリーズ	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	はい: • WX3510H • WX3520H • WX3540H • WX3520H-F ×:WX3508H
WX5500Eシリーズ	WX5 510E WX5 540E	EWP-WX5510E EWP-WX5540E	はい
WX5500Hシリーズ	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	はい
アクセスコントローラモジュール	LSUM1WCM E0EWPXM1 WCME0 LSQM1WCMX20 LSUM1WCMX 20RT LSQM1WCMX 40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0EW PXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	はい: • LSQMーWCMX四〇 • LSUM1WCMX40RT いいえ: • LSUM1WCME0 • EWPXM1WCME0 • LSQM1WCMX20 • LSUM1WCMX20RT
WX1800Hシリーズ	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	いいえ
WX3800Hシリーズ	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	はい
WX5800Hシリーズ	WX5860H	EWP-WX5860H-GL	はい • EWPXM2WCMD0F EWPXM1MAC0F

制限事項およびガイドライン

AC間ローミング認証とMACベースのクイックポータル認証の両方を設定しないでください。

この機能は、Webページ上でポータル認証を実行するポータルユーザーに対してのみ有効です。

手順

1. システムビューに入ります。

system-view

2. ポータルローミングセンターを作成し、そのビューに入ります。

   portal roaming-center

3. WLANローミングセンターと通信するためのIPv4アドレスを指定します。

   ip ip-address

   既定では、WLANローミングセンターと通信するためのIPv4アドレスは指定されていません。

4. WLANローミングセンターと通信するためのIPv6アドレスを指定します。

   ipv6 ipv6-address

   既定では、WLANローミングセンターと通信するためのIPv6アドレスは指定されていません。

5. WLANローミングセンターと通信するためのUDPポート番号を指定します。

   port port-number

   デフォルトでは、UDPポート60035は、ポータルローミングセンターがWLANローミングセンターと通信するために使用されます。

6. (任意)WLANローミングセンターからの応答の待機タイマーを設定します。

   response-timeout timeout

   デフォルトでは、待機タイマーは3秒です。

7. (任意)ポータルローミングセンターがWLANローミングセンターにパケットを送信する最大試行回数を設定します。

   retry retries

   デフォルトでは、パケット転送の最大試行回数は5回です。

8. (任意)ポータルローミングセンターがユーザートラフィックを拒否できるようにします。

   user-traffic deny

   既定では、ポータルローミングセンターはユーザートラフィックを拒否しません。

9. ポータルローミングセンターを有効にします。

   roaming-center enable

   既定では、ポータルローミングセンターは無効になっています。

ポータルフェール許可機能の設定

このタスクについて

インターフェイスまたはサービステンプレートにポータルフェール許可機能を設定できます。アクセスデバイスは、ポータル認証サーバーまたはポータルWebサーバーが到達不能であることを検出すると、ポータル認証なしでユーザーにネットワークアクセスを許可します。

ポータル認証サーバーとポータルWebサーバーの両方でfail-permitをイネーブルにした場合、デバイスは次の処理を実行します。

- ポータル認証サーバーが到達不能であるか、すべてのポータルWebサーバーが到達不能である場合に、ポータル認証を無効にします。
- ポータル認証とWebサーバーの両方に到達可能な場合は、ポータル認証を再開します。

ポータル認証が再開された後、非認証ユーザーはネットワークにアクセスするためにポータル認証を通過する必要があります。fail-permitイベントの前にポータル認証を通過したユーザーは、ネットワークへのアクセスを継続できます。

インターフェイス上でのポータルフェール許可の設定

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. インターフェイス上のポータル認証サーバーに対して、portal fail-permitをイネーブルにします。

   portal [ipv6] fail-permit server server-name

   デフォルトでは、インターフェイス上のポータル認証サーバーに対して、portal fail-permitはディセーブルになっています。
4. インターフェイス上でポータルWebサーバーのportal fail-permitをイネーブルにします。

   portal [ipv6] fail-permit web-server

   デフォルトでは、インターフェイス上のポータルWebサーバーに対して、portal fail-permitはディセーブルです。

サービステンプレートでのポータルフェール許可の設定

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. サービステンプレート上のポータルWebサーバーのポータルフェール許可をイネーブルにします。

   portal [ipv6] fail-permit web-server

   デフォルトでは、サービステンプレート上のポータルWebサーバーに対してポータルフェール許可がディセーブルになっています。

NAS-Port-Type属性の設定

このタスクについて

RADIUS要求で伝送されるNAS-Port-Type属性は、ユーザーのアクセスインターフェイスタイプを表します。

アクセスデバイスとして、BASとポータルクライアントの間に複数のネットワークデバイスが存在する場合、BASはユーザーのインターフェイスタイプを正しく取得できない場合があります。たとえば、ワイヤレスポータルユーザーのためにBASによって取得されるアクセスインターフェイスタイプは、有線インターフェイスのタイプである場合があります。

ユーザーを認証しました。BASが正しいユーザーインターフェイスタイプをRADIUSサーバーに送信するには、次の作業を実行して正しいNAS-Port-Type値を指定します。

ポータルユーザーがインターフェイスまたはサービステンプレートからログインする場合、NAS-Port-Type属性の値は次のようになります。

- NAS-Port-Typeが設定されている場合、NAS-Port-Typeの値は設定された値になります。
- NASポートタイプが構成されていない場合、NASポートタイプの値は、アクセスデバイスによって取得されたユーザーのアクセスインターフェイスタイプです。

インターフェイスでのNAS-Port-Typeアトリビュートの設定

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

interface interface-type interface-number

3. インターフェイス上でNAS-Port-Typeアトリビュートを設定します。

   portal nas-port-type { ethernet | wireless }

   デフォルトでは、RADIUS要求で伝送されるポータルのNAS-Port-Type属性は、アクセスデバイスによって取得されるユーザーのアクセスインターフェイスタイプ値です。

サービステンプレートのNASポートタイプ属性の構成

1. システムビューに入ります。

   system-view

2. サービステンプレートビューに入ります。

   wlan service-template service-template-name

3. インターフェイス上でNAS-Port-Typeアトリビュートを設定します。

   portal nas-port-type { ethernet | wireless }

   デフォルトでは、RADIUS要求で伝送されるポータルのNAS-Port-Type属性は、アクセスデバイスによって取得されるユーザーのアクセスインターフェイスタイプ値です。

ワイヤレスクライアントでの有効性チェックの有効化

このタスクについて

サービステンプレートでポータル認証が有効になっている場合は、この機能を有効にします。APがクライアントトラフィックを転送するワイヤレスネットワークでは、ACはクライアントのARPエントリを持っていません。したがって、ACはARPエントリを使用してポータルクライアントの有効性をチェックできません。有効なユーザーがポータル認証を実行できるようにするには、ACでワイヤレスクライアントの有効性チェックを有効にする必要があります。

この機能を使用すると、WLANスヌーピングテーブル、DHCPスヌーピングテーブル、およびARPテーブル内のクライアント情報を検索することによって、ACはクライアントを検証できます。クライアント情報が存在する場合、ACはクライアントがポータル認証に有効であると判断します。

制限事項およびガイドライン

サービステンプレートでポータル認証がイネーブルになっている場合は、この機能をイネーブルにする必要があります。

手順

1. システムビューに入ります。

   system-view

2. ワイヤレスポータルクライアントで妥当性チェックを有効にします。

   portal host-check enable

   デフォルトでは、ワイヤレスポータルクライアントの有効性チェックはディセーブルになっています。デバイスは、ARPエントリのみに従ってワイヤレスポータルクライアントの有効性をチェックします。

ポータル検出機能の設定

ポータルユーザーのオンライン検出の構成

このタスクについて

オンライン検出機能を使用すると、ポータルユーザーの異常なログアウトを迅速に検出できます。IPv4ポータルユーザーに対してARPまたはICMP検出を構成します。IPv6ポータルユーザーに対してNDまたはICMPv6検出を構成します。

アイドル時間内にポータルユーザーからパケットを受信しなかった場合、デバイスはユーザーのオンラインステータスを次のように検出します。

- ICMPまたはICMPv6検出ユーザーステータスを検出するために、設定可能な間隔でICMPまたはICMPv6要求をユーザーに送信します。
  - 最大検出試行回数以内にデバイスが応答を受信した場合、デバイスはユーザーがオンラインであると見なし、検出パケットの送信を停止します。次に、デバイスはアイドルタイマーをリセットし、タイマーが期限切れになると検出プロセスを繰り返します。
  - 最大数の検出試行後にデバイスが応答を受信しなかった場合、デバイスはユーザーをログアウトさせます。
- ARPまたはND検出:ARPまたはND要求をユーザーに送信し、設定可能な間隔でユーザーのARPまたはNDエントリステータスを検出します。
  - 最大検出試行回数以内にユーザーのARPまたはNDエントリが更新された場合、デバイスはユーザーがオンラインであると見なして検出を停止します。次に、デバイスはアイドルタイマーをリセットし、タイマーが期限切れになると検出プロセスを繰り返します。
  - 最大数の検出試行後にユーザーのARPまたはNDエントリが更新されない場合、デバイスはユーザーをログアウトします。

制限事項およびガイドライン

ARP検出およびND検出は、直接ポータル認証にのみ適用されます。ICMP検出は、すべてのポータル認証モードに適用されます。

手順

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. ポータルユーザーのオンライン検出を構成します。

   IPv4:

   portal user-detect type { **arp** | i**cmp } [retry** *retries*] [**interval** *interva*l] [**idle** *time*]

   IPv6:

   portal ipv6 user-detect type { **icmpv6 | nd } [retry** *retries*] [**interval** *interval*] [**idle** *time*]

   デフォルトでは、オンライン検出はインターフェイス上のポータルユーザーに対してディセーブルです。

ポータル認証サーバー検出の構成

このタスクについて

ポータル認証中に、アクセスデバイスとポータル認証サーバー間の通信が切断されると、新規新規ポータルユーザーはログインできません。オンラインポータルユーザーは正常にログアウトできません。

この問題に対処するには、アクセスデバイスがポータルサーバーの到達可能性の変化を迅速に検出し、その変化に対応するアクションを実行できる必要があります。

ポータル認証サーバー検出機能を使用すると、デバイスは、ポータル認証サーバーによって送信されたポータルパケットを定期的に検出して、サーバーの到達可能性を判断できます。デバイスが検出タイムアウト(タイムアウトタイムアウト)内にポータルパケットを受信し、ポータルパケットが有効である場合、デバイスはポータル認証サーバーが到達可能であると見なします。それ以外の場合、デバイスはポータル認証サーバーが到達不能であると見なします。

ポータルパケットには、ユーザーログインパケット、ユーザーログアウトパケットおよびハートビートパケットが含まれます。ハートビートパケットはサーバーによって定期的に送信されます。ハートビートパケットを検出することにより、デバイスは他のポータルパケットを検出するよりも迅速にサーバーの実際のステータスを検出できます。

制限事項およびガイドライン

ポータル認証サーバー検出機能は、デバイスにポータル対応のインターフェイスがある場合にだけ有効になります。

ハートビートパケットの送信をサポートしているのは、iMCポータル認証サーバーだけです。ハートビートパケットを検出してサーバーの到達可能性をテストするには、iMCポータル認証サーバーでサーバーハートビート機能をイネーブルにする必要があります。

サーバーの到達可能性ステータスが変化したときに、次の1つまたは複数のアクションを実行するようにデバイスを設定できます。

- NMSへのトラップメッセージの送信。このトラップメッセージには、ポータル認証サーバーの名前と現在の状態が含まれます。
- ポータル認証サーバーの名前、現在の状態、および元の状態を含むログメッセージを送信する。
- ポータル失敗許可を有効にします。ポータル認証サーバーが到達不能の場合、インターフェイス上のポータル失敗許可機能により、インターフェイス上のユーザーはネットワークにアクセスできます。サーバーが回復すると、インターフェイス上のポータル認証が再開されます。詳細は、「ポータル失敗許可機能の構成」を参照してください。

デバイスに設定されている検出タイムアウトが、ポータル認証サーバーに設定されているサーバーのハートビート間隔より大きいことを確認します。

手順

1. システムビューに入ります。

   system-view
2. ポータル認証サーバービューに入ります。

   portal server server-name
3. ポータル認証サーバーの検出を構成します。

   server-detect [timeout *timeout*] { **log | trap** } *

   デフォルトでは、ポータル認証サーバーの検出はディセーブルです。

ポータルWebサーバー検出の構成

このタスクについて

アクセスデバイスとポータルWebサーバー間の通信が切断されている場合、ポータル認証プロセスを完了できません。この問題に対処するには、アクセスバイスでポータルWebサーバー検出を有効にします。

ポータルWebサーバー検出機能を使用すると、アクセスデバイスはWebアクセスプロセスをシミュレートして、ポータルWebサーバーへのTCP接続を開始します。TCP接続が正常に確立されると、アクセスデバイスは検出が成功したとみなし、ポータルWebサーバーに到達可能であるとみなします。それ以外の場合は、検出が失敗したとみなします。アクセスデバイスのインターフェイス上のポータル認証ステータスは、ポータルWebサーバー検出機能に影響しません。

次の検出パラメータを設定できます。

- Detection interval: デバイスがサーバーの到達可能性を検出する間隔。
- 連続した失敗の最大数: 連続した検出失敗の数がこの値に達すると、アクセス装置はポータルWebサーバーが到達不能であると見なします。

サーバーの到達可能性ステータスが変化したときに、次の1つまたは複数のアクションを実行するようにデバイスを設定できます。

- トラップメッセージをNMSに送信します。トラップメッセージには、ポータルWebサーバーの名前と現在の状態が含まれます。
- ポータルWebサーバーの名前、現在の状態、および元の状態を含むログメッセージを送信する。
- ポータル失敗許可を使用可能にします。ポータルWebサーバーが到達不能の場合、インターフェイス上のポータル失敗許可機能により、インターフェイス上のユーザーはネットワークアクセスを許可されます。サーバーが回復すると、インターフェイス上のポータル認証が再開されます。詳細は、「ポータル失敗許可機能の構成」を参照してください。

制限事項およびガイドライン

ポータルWebサーバー検出機能は、ポータルWebサーバーのURLが指定されていて、デバイスにポータル対応のインターフェイスがある場合にのみ有効になります。

手順

1. システムビューに入ります。

   system-view
2. ポータルWebサーバービューに入ります。

   portal web-server server-name
3. ポータルWebサーバー検出を構成します。

   server-detect [**interval** *interval*] [**retry** *retries*] { **log | trap** } *

   デフォルトでは、ポータルWebサーバーの検出は無効になっています。
4. ポータルWebサーバー検出のURLおよびタイプを構成します。

   server-detect url *string* [**detect-type { http | tcp** }]

   デフォルトでは、ポータルWebサーバー検出のURLはポータルWebサーバーのURLです。ポータルWebサーバー検出のタイプはTCP検出です。

DHCPパケットキャプチャのイネーブル化

このタスクについて

この機能により、ACは、ポータルユーザーのDHCPパケットをキャプチャすることによって、ポータルユーザーのオンラインステータスを検出できます。

この機能がイネーブルの場合、ACはポータルユーザーとDHCPサーバー間のDHCPパケットをキャプチャし、ユーザーのIPアドレスリース情報を取得します。次に、ACは次のようにポータルユーザーのオンラインステータスを検出します。

- リースが期限切れになる前にACがポータルユーザーからDHCPリース更新パケットをキャプチャした場合、ACはポータルユーザーがオンラインであると判断します。
- リースが期限切れになる前にDHCPリース更新パケットがキャプチャされない場合、ACはポータルユーザーを強制的にログアウトします。

DHCP パケットの詳細については、Network Connectivity Configuration Guide の「DHCP configuration」を参照してください。

DHCPパケットキャプチャタイマーのタイムアウト時間は、DHCPパケット内のIPアドレスリース時間と同じです。このタイマーは、DHCPパケットがキャプチャされるたびにリセットされます。

手順

1. システムビューに入ります。

   system-view
2. DHCPパケットキャプチャをイネーブルにして、ポータルユーザーのオンラインステータスを検出します。

   portal idle-cut dhcp-capture enable

   デフォルトでは、DHCPパケットキャプチャはディセーブルになっています。

ポータルユーザーの同期の構成

このタスクについて

アクセスデバイスがポータル認証サーバーとの通信を失うと、通信が再開された後で、アクセスデバイスおよびポータル認証サーバーのポータルユーザー情報に一貫性がなくなる場合があります。この問題に対処するために、デバイスにはポータルユーザー同期機能が用意されています。この機能は、次のようにポータル同期パケットを送信および検出することによって実装されます。

1. ポータル認証サーバーは、ユーザーのハートビート間隔で、オンラインユーザー情報を同期パケットでアクセスデバイスに送信します。

   ユーザーのハートビート間隔は、ポータル認証サーバーで設定されます。
2. アクセスデバイスは、同期パケットを受信すると、パケットに含まれるユーザーと自身のユーザーリストを比較し、次の処理を実行します。
   - パケットに含まれるユーザーがアクセスデバイス上に存在しない場合、アクセスデバイスはポータル認証サーバーにユーザーを削除するよう通知します。アクセスデバイスは、ユーザーがログインするとすぐに同期検出タイマー(タイムアウトタイムアウト)を開始します。
   - ユーザーが同期検出間隔内のどの同期パケットにも現れない場合、アクセスデバイスは、ユーザーがポータル認証サーバー上に存在しないと見なし、ユーザーをログアウトさせます。

制限事項およびガイドライン

ポータルユーザーの同期化では、ポータルユーザーのハートビート機能をサポートするポータル認証サーバーが必要です。ポータルユーザーのハートビート機能をサポートするのは、iMCポータル認証サーバーのみです。ポータルユーザーの同期化機能を実装するには、ポータル認証サーバーでユーザーのハートビート機能も構成する必要があります。ポータル認証サーバーで構成されたユーザーのハートビート間隔が、アクセスデバイスで構成された同期検出タイムアウトより大きくないことを確認してください。

アクセスデバイス上のポータル認証サーバーを削除すると、ポータル認証サーバーのユーザー同期設定も削除されます。

手順

1. システムビューに入ります。

   system-view
2. ポータル認証サーバービューに入ります。

   portal server server-name
3. ポータルユーザーの同期を構成します。

   user-sync timeout timeout

   デフォルトでは、ポータルユーザーの同期は無効になっています。

ポータルパケット属性の設定

BAS-IPまたはBAS-IPv6アトリビュートの設定

このタスクについて

デバイスがPortal2.0を実行する場合、ポータル認証サーバーに送信される非送信請求パケットは、BAS-IPアトリビュートを伝送する必要があります。デバイスがPortal3.0を実行する場合、ポータル認証サーバーに送信される非送信請求パケットは、BAS-IPまたはBAS-IPv6アトリビュートを伝送する必要があります。

このアトリビュートの設定後、デバイスがポータル認証サーバーに送信する非送信請求通知ポータルパケットの送信元IPアドレスは、設定されたBAS-IPまたはBAS-IPv6アドレスになります。アトリビュートが設定されていない場合、ポータルパケットの送信元IPアドレスはパケット出力インターフェイスのIPアドレスになります。

制限事項およびガイドライン

必須ユーザーのログアウトプロセス中に、デバイスはポータル通知パケットをポータル認証サーバーに送信します。認証またはログアウトプロセスを完了するには、BAS-IPまたはBAS-IPv6属性がポータル認証サーバーで指定されたデバイスIPアドレスと同じであることを確認してください。

次の条件が満たされている場合は、ポータル認証対応インターフェイスでBAS-IPまたはBAS-IPv6アトリビュートを設定する必要があります。

- ポータル認証サーバーは、H3C iMCサーバーです。
- ポータル認証サーバーで指定されたポータルデバイスのIPアドレスは、ポータルパケット出力インターフェイスのIPアドレスではありません。

インターフェイスでのBAS-IPまたはBAS-IPv6アトリビュートの設定

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. BAS-IPまたはBAS-IPv6アトリビュートを設定します。

   IPv4:

   portal bas-ip ipv4-address

   デフォルトでは、IPv4ポータル応答パケットのBAS-IPアトリビュートはパケットの送信元IPv4アドレスです。IPv4ポータル通知パケットのBAS-IPアトリビュートはパケットの出力インターフェイスのIPv4アドレスです。

IPv6:

portal bas-ipv6 ipv6-address

デフォルトでは、IPv6ポータル応答パケットのBAS-IPv6アトリビュートはパケットの送信元IPv6アドレスです。IPv6ポータル通知パケットのBAS-IPv6アトリビュートはパケットの出力インターフェイスのIPv6アドレスです。

サービステンプレートでのBAS-IPアトリビュートの設定

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. BAS-IPまたはBAS-IPv6アトリビュートを設定します。

   IPv4:

   portal bas-ip ipv4-address

   デフォルトでは、IPv4ポータル応答パケットのBAS-IPアトリビュートはパケットの送信元IPv4アドレスです。IPv4ポータル通知パケットのBAS-IPアトリビュートはパケットの出力インターフェイスのIPv4アドレスです。

   IPv6:

   portal bas-ipv6 ipv6-address

   デフォルトでは、IPv6ポータル応答パケットのBAS-IPv6アトリビュートはパケットの送信元IPv6アドレスです。IPv6ポータル通知パケットのBAS-IPv6アトリビュートはパケットの出力インターフェイスのIPv6アドレスです。

デバイスIDの指定

このタスクについて

ポータル認証サーバーは、デバイスIDを使用して、プロトコルパケットをポータルサーバーに送信するデバイスを識別します。

制限事項およびガイドライン

設定されたデバイスIDが、同じポータル認証サーバーと通信する他のアクセスデバイスと異なることを確認します。

手順

1. システムビューに入ります。
   System-view
2. デバイスIDを指定します。

   portal device-id device-id

   デフォルトでは、デバイスにはデバイスIDが設定されていません。

RADIUSパケットのアトリビュートの設定

NAS-Port-Id属性のフォーマットの指定

このタスクについて

異なるベンダーのRADIUSサーバーでは、RADIUSパケット内のNAS-Port-Id属性のフォーマットが異なる場合があります。必要に応じてNAS-Port-Id属性のフォーマットを指定できます。

デバイスは事前定義されたフォーマット(フォーマット1、2、3および4)をサポートしています。フォーマットの詳細は、「ユーザーアクセスおよび認証コマンドリファレンス」のポータルコマンドを参照してください。

手順

1. システムビューに入ります。

   system-view

2. NAS-Port-Id属性の形式を指定します。

   portal *nas-port-id* **format** { 1 | 2 | 3 | 4 }

   デフォルトでは、NAS-Port-Idアトリビュートのフォーマットはformat2です。

インターフェイスへのNAS-IDプロファイルの適用

このタスクについて

デフォルトでは、デバイスはすべてのRADIUS要求のNAS-Identifierアトリビュートでデバイス名を送信します。

NAS-IDプロファイルを使用すると、異なるVLANからのRADIUS要求で異なるNAS-Identifier属性文字列を送信できます。文字列は、管理要件に応じて、組織名、サービス名、または任意のユーザー分類基準になります。

たとえば、NAS-ID companyAを会社Aのすべてのvlanにマッピングします。デバイスは、会社Aユーザーからの要求を識別するために、RADIUSサーバーのNAS-Identifierアトリビュートで会社Aを送信します。

制限事項およびガイドライン

NAS-IDプロファイルをポータル対応のインターフェイスに適用できます。インターフェイスにNAS-IDプロファイルが指定されていない場合、または指定されたプロファイルに一致するNAS-IDが見つからない場合、デバイスはインターフェイスNAS-IDとしてデバイス名を使用します。

手順

1. システムビューに入ります。

   system-view

2. NAS-IDプロファイルを作成して、NAS-IDプロファイルビューに入ります。

   aaa nas-id profile profile-name

   このコマンドの詳細については、『User Access and Authentication Command Reference』の「AAAコマンド」を参照してください。

3. プロファイルにNAS IDおよびVLANバインディングを設定します。

   nas-id nas-identifier bind vlan vlan-id

   このコマンドの詳細については、『User Access and Authentication Command Reference』の「AAAコマンド」を参照してください。

4. インターフェイス上のNAS-IDプロファイルを指定します。

   a. システムビューに戻ります。

      quit

b. レイヤー3 interfaceビューに入ります。

interface interface-type interface-number

c. インターフェイス上のNAS-IDプロファイルを指定します。

portal nas-id-profile profile-name

ユーザートラフィックバックアップしきい値の設定

このタスクについて

ユーザーのトラフィックがユーザートラフィックバックアップのしきい値に達すると、デバイスはユーザーのトラフィックをバックアップします。しきい値を小さくすると、ユーザートラフィックのバックアップがより正確になります。ただし、多数のユーザーが存在する場合、しきい値が小さくなるとユーザートラフィックのバックアップが頻繁に行われ、ユーザーのオンライン、オフラインおよび会計プロセスに影響が及びます。サービスパフォーマンスとトラフィックバックアップの精度のバランスを取るために、適切なしきい値を設定します。

手順

1. システムビューに入ります。

system-view

2. ユーザートラフィックバックアップのしきい値を設定します。

portal traffic-backup threshold value

デフォルトでは、ユーザートラフィックバックアップのしきい値は10MBです。

MACベースのクイックポータル認証の構成

MACベースのクイックポータル認証の設定に関する制約事項およびガイドライン

MACベースのクイックポータル認証とAC間ローミングの両方を設定しないでください。

MACベースのクイックポータル認証をサポートするのは、IPv4直接認証だけです。

ポータル事前認証ドメインが設定されたインターフェイスでMACベースのクイックポータル認証を有効にするには、free-trafficしきい値を0バイトに設定します。

リモートMACバインディングサーバーの設定

このタスクについて

デバイス上に複数のMACバインディングサーバーを設定できます。

サーバーのIPアドレスポート番号や空きトラフィックのしきい値などのMACバインディングサーバーパラメータを設定するには、次の作業を実行します。

手順

1. システムビューに入ります。

system-view

2. MACバインディングサーバーを作成し、そのビューに入ります。

   portal mac-trigger-server server-name

3. MACバインディングサーバーを設定します。
   - MACバインディングサーバーのIPアドレスを指定します。

     ip *ipv4-address* [**key** { **cipher | simple** } *string*]

     デフォルトでは、MACバインディングサーバーにIPアドレスは指定されていません。
   - (任意)MACバインディングサーバーがMACバインディングクエリーパケットをリッスンするUDPポート番号を設定します。

     port port-number

     デフォルトでは、MACバインディングサーバーはUDPポート50100でMACバインディングクエリーパケットをリッスンします。
   - (任意)MACバインディングサーバーにMACバインディングクエリーを送信する最大試行回数と間隔を設定します。

     binding-retry { *retries* | **interval** *interval* } *

     デフォルトでは、クエリーの最大試行回数は3回で、クエリー間隔は1秒です。
   - (任意)MACバインディングサーバーのタイプを指定します。

     server-type { cmcc | imc }

     デフォルトでは、MACバインディングサーバーのタイプはiMCです。
4. (任意)フリートラフィックのしきい値を設定します。

   free-traffic threshold value

   デフォルトでは、空きトラフィックのしきい値は0バイトです。
5. (任意)RADIUSサーバーに送信されるRADIUS要求で伝送されるNASポートタイプの値を設定します。

   nas-port-type value

   デフォルトでは、RADIUS要求で伝送されるNASポートタイプの値は19です。
6. (任意)ポータルプロトコルのバージョンを指定します。

   version version-number

   デフォルトでは、ポータルプロトコルのバージョンは1です。
7. (任意)MACバインディングクエリー応答を受信した後、デバイスがポータル認証の完了を待機するタイムアウトを設定します。

   authentication-timeout minutes

   デフォルトでは、ポータル認証のタイムアウト時間は3分です。
8. (任意)MACトリガーエントリのエージングタイムを設定します。

   aging-time seconds

   デフォルトでは、MACトリガーエントリのエージングタイムは300秒です。
9. (任意)AAA失敗アンバインドをイネーブルにします。

   aaa-fail nobinding enable

   デフォルトでは、AAA失敗アンバインドはディセーブルです。

ローカルMACバインディングサーバーの設定

このタスクについて

ローカルポータルユーザーにMACベースのクイックポータル認証を提供するには、アクセスデバイスがローカルMACバインディングサーバーとして動作するように、次の作業を実行します。

デバイスに複数のローカルMACバインディングサーバーを設定できます。各サーバーに対して、ローカルMACベースのクイックポータル認証に関連するパラメータを設定できます。

手順

1. システムビューに入ります。
   system-view
2. MACバインディングサーバーを作成し、そのビューに入ります。
   portal mac-trigger-server server-name
3. ローカルMACベースのクイックポータル認証をイネーブルにします。
   local-binding enable
   デフォルトでは、ローカルMACベースのクイックポータル認証はディセーブルです。
4. (任意)フリートラフィックのしきい値を設定します。
   free-traffic threshold value
   デフォルトでは、空きトラフィックのしきい値は0バイトです。
5. (任意)ローカルMACアカウントバインディングエントリのエージングタイムを設定します。
   local-binding aging-time minutes
   デフォルトでは、ローカルMACアカウントバインディングエントリのエージングタイムは720分です。
6. (任意)MACトリガーエントリのエージングタイムを設定します。
   aging-time seconds
   デフォルトでは、MACトリガーエントリのエージングタイムは300秒です。
7. (任意)AAA失敗アンバインドをイネーブルにします。
   aaa-fail nobinding enable
   デフォルトでは、AAA失敗アンバインドはディセーブルです。

インターフェイス上のMACバインディングサーバーの指定

このタスクについて

インターフェイス上でMACバインディングサーバーを指定した後、デバイスはインターフェイス上のポータルユーザーに対してMACベースのクイックポータル認証を実装できます。

手順

1. システムビューに入ります。
   system-view
2. レイヤ3インターフェースビューに入ります。
   interface interface-type interface-number
3. インターフェイス上のMACバインディングサーバーを指定します。
   portal apply mac-trigger-server server-name

デフォルトでは、インターフェイスにMACバインディングサーバーは指定されていません。

サービステンプレートでのMACバインディングサーバーの指定

このタスクについて

MACバインディングサーバーがサービステンプレートで指定された後、デバイスは、サービステンプレートを使用するポータルユーザーに対して、MACベースのクイックポータル認証を実装できます。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template service-template-name
3. サービステンプレート上のMACバインディングサーバーを指定します。
   portal apply mac-trigger-server server-name
   デフォルトでは、サービステンプレートにMACバインディングサーバーは指定されていません。

クラウドMACトリガー認証を設定する

このタスクについて

この機能により、クラウドポータルサーバーはMACバインディングサーバーとして機能し、ポータルユーザーに対してクラウドMACトリガー認証を実行できます。

手順

1. システムビューに入ります。
   system-view
2. MACバインディングサーバーを作成し、そのビューに入ります。
   portal mac-trigger-server server-name
3. クラウドMACトリガー認証をイネーブルにします。
   cloud-binding enable
   デフォルトではクラウドMACトリガー認証はディセーブルです。
4. クラウドポータル認証サーバーのURLを指定します。
   cloud-server url url-string
   デフォルトでは、クラウドポータルの認証サーバーのURLは指定されていません。デバイスは、ポータルのWebサーバーのURLをクラウドポータルの認証サーバーのURLとして使用します。

ポータルクライアントのルールARPまたはNDエントリ機能を無効にする

このタスクについて

ルールARPまたはNDエントリ機能がポータルクライアントに対して有効になっている場合、ポータルクライアントのARPまたはNDエントリは、クライアントがオンラインになった後のルールエントリです。ルー

ルエントリは期限切れになることはなく、ポータルクライアントがオフラインになった直後に削除されます。ARPまたはNDエントリがクライアントに対して再学習される前にポータルクライアントがオフラインになり、オンラインになろうとすると、クライアントは認証に失敗します。このような認証の失敗を回避するには、この機能を無効にしてください。ポータルクライアントのARPまたはNDエントリは、クライアントがオンラインになった後の動的エントリであり、期限切れになったときにのみ削除されます。

制限事項およびガイドライン

この機能をイネーブルまたはディセーブルにしても、既存のルール/ダイナミックARPまたはNDエントリには影響しません。

手順

1. システムビューに入ります。

   system-view
2. ポータルクライアントのルールARPまたはNDエントリ機能を無効にします。

   undo portal refresh { arp | nd } enable

   デフォルトでは、ルールARPまたはNDエントリ機能はポータルクライアントに対して無効になっています。

ポータルユーザーのトラフィックアカウンティングの無効化

このタスクについて

アカウンティングサーバーは、時間ベースまたはトラフィックベースのアカウンティングを実行する場合と、アカウンティングを実行しない場合があります。

アカウンティングサーバーがトラフィックベースのアカウンティングを実行しない場合は、デバイス上のポータルユーザーに対してトラフィックアカウンティングをディセーブルにします。デバイスはポータルユーザーに対して迅速なアカウンティングを提供し、トラフィック統計情報は不正確になります。

アカウンティングサーバーがトラフィックベースのアカウンティングを実行する場合は、ポータルユーザーのトラフィックアカウンティングをイネーブルにします。デバイスは、ポータルユーザーに正確なトラフィック統計情報を提供します。

手順

1. システムビューに入ります。

   system-view
2. ポータルユーザーのトラフィックアカウンティングをディセーブルにします。

   portal traffic-accounting disable

   デフォルトでは、トラフィックアカウンティングはポータルユーザーに対してイネーブルです。

ワイヤレスポータルユーザーを自動的にログアウトする

このタスクについて

この機能を有効にすると、ワイヤレスクライアントがネットワークから切断された後、デバイスは自動的にポータルユーザーをログアウトします。

手順

1. システムビューに入ります。

   system-view

2. ワイヤレスポータルユーザーの自動ログアウトを有効にします。

   portal user-logoff after-client-offline enable

   デフォルトでは、ワイヤレスクライアントがネットワークから切断された後、デバイスはポータルユーザーを自動的にログアウトしません。

Webリダイレクトの設定

Webリダイレクトについて

Webリダイレクトは簡素化されたポータル機能です。Webリダイレクトを使用すると、ユーザーはポータル認証を実行しませんが、ブラウザでの最初のWebアクセス試行時に指定されたURLに直接リダイレクトされます。指定されたリダイレクト間隔の後、ユーザーは再び訪問中のWebサイトから指定されたURLにリダイレクトされます。

WebリダイレクトはISPに拡張サービスを提供できます。たとえば、ISPはリダイレクトされたWebページに広告を出したり、情報を公開したりできます。

インターフェイスでのWebリダイレクトの設定

制限事項およびガイドライン

Webリダイレクト機能は、デフォルトポート番号80を使用するHTTPパケットに対してだけ有効です。

デバイスURLをWebリダイレクトURLとして使用する場合、またはユーザーがデバイスURLに正常にアクセスできるようにする場合は、HTTPサービスをイネーブルにする必要があります。HTTPサービスをイネーブルにするには、ip http enableコマンドを使用します。

インターフェイス上でWebリダイレクトおよびポータル認証がすべてイネーブルになっている場合、デバイスはインターフェイス上のユーザーを次のようにリダイレクトします。

- デバイスは、ユーザーの最初のHTTPリクエストを指定されたURLにリダイレクトします。次に、デバイスはユーザーの次のHTTPリクエストをポータル認証ページにリダイレクトします。ユーザーがログアウトした後、ユーザーは最初のWebアクセスで再び指定されたURLにリダイレクトされます。
- 指定したリダイレクト間隔の後、ユーザーがオンラインかどうかにかかわらず、ユーザーは指定したURLにリダイレクトされます。このプロセスでは、オンラインユーザーがオフラインになることはありません。

手順

1. システムビューに入ります。

   system-view

2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number

3. Webリダイレクトを設定します。

   web-redirect [**ipv6**] **url** *url-string* [**interval** *interval*]

   既定では、Webリダイレクトは無効になっています。

サービステンプレートでのWebリダイレクトの設定

制限事項およびガイドライン

Webリダイレクト機能は、デフォルトポート番号80を使用するHTTPパケットに対してだけ有効です。

デバイスURLをWebリダイレクトURLとして使用する場合、またはユーザーがデバイスURLに正常にアクセスできるようにする場合は、HTTPサービスをイネーブルにする必要があります。HTTPサービスをイネーブルにするには、ip http enableコマンドを使用します。

サービステンプレートでWebリダイレクト認証とポータル認証の両方を有効にしないでください。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. サービステンプレートでWebリダイレクトを設定します。

   web-redirect [**ipv6**] **url** *url-string* [**interval** *interval*]

   既定では、Webリダイレクトはサービステンプレートでは無効になっています。

ポータルセーフリダイレクトの設定

このタスクについて

Portal safe-redirectは、HTTPリクエストをHTTPリクエストメソッド、ブラウザータイプ(HTTP User Agent内)および宛先URLでフィルタし、許可されたHTTPリクエストのみをリダイレクトします。これにより、過負荷のためにポータルWebサーバーがHTTPリクエストに応答できないリスクが軽減されます。

表2ポータルセーフリダイレクトでサポートされるブラウザータイプ

ブラウザの種類	説明説明
Safari	Appleブラウザ
Chrome	Googleブラウザ
Firefox	Firefoxブラウザ
UC	UCブラウザ
QQブラウザ	QQブラウザ
LBBROWSER	Cheetahブラウザ
TaoBrowser	Taobaoブラウザ
Maxthon	Maxthonブラウザ
BIDUBrowser	Baiduブラウザ

MSIE10.0	Microsoft IE10.0ブラウザ
MSIE9.0	Microsoft IE9.0ブラウザ
MSIE8.0	Microsoft IE8.0ブラウザ
MSIE7.0	Microsoft IE7.0ブラウザ
MSIE6.0	Microsoft IE6.0ブラウザ
MetaSr	Sogouブラウザ

手順

1. システムビューに入ります。

   system-view
2. ポータルセーフリダイレクトを有効にします。

   portal safe-redirect enable

   デフォルトでは、ポータルのセーフリダイレクト機能はディセーブルです。
3. (任意)ポータルのsafe-redirectによって許可されるHTTP要求方式を指定します。

   portal safe-redirect method { get | post }

   デフォルトでは、ポータルのsafe-redirectがイネーブルになった後、デバイスはGET方式を使用してHTTP要求だけをリダイレクトできます。
4. (任意)ポータルセーフリダイレクトによって許可されるブラウザータイプを指定します。

   portal safe-redirect user-agent user-agent-string

   デフォルトでは、ブラウザータイプは指定されていません。ポータルセーフリダイレクトが有効になった後、デバイスは、サポートされているすべてのブラウザ(表2を参照)によって送信されたHTTP要求をリダイレクトできます。
5. (任意)ポータルのsafe-redirectによって禁止されるURLを設定します。

   portal safe-redirect forbidden-url user-url-string

   デフォルトでは、禁止URLは設定されていません。デバイスは任意のURLを使用してHTTP要求をリダイレクトできます。
6. (任意)portal safe-redirectによって禁止されるファイル名拡張子を設定します。

   portal safe-redirect forbidden-file filename-extension

   デフォルトでは、禁止ファイル名拡張子は設定されていません。デバイスは、URL内のファイル拡張子に関係なくHTTP要求をリダイレクトします。
7. (任意)portal safe-redirectのデフォルトアクションを設定します。

   portal safe-redirect default-action { forbidden | permit }

   デフォルトでは、ポータルのsafe-redirectに対するデフォルトアクションは設定されていません。
8. ポータルセーフリダイレクトによって許可されるURLを設定します。

   portal safe-redirect permit-url user-url-string

   デフォルトでは、ポータルセーフリダイレクトで許可されるURLは構成されません。デバイスは、URLを使用してWebリクエストをリダイレクトします。

単一ユーザーのポータルリダイレクトセッションの最大数の設定

このタスクについて

ユーザークライアントが悪質なソフトウェアまたはウイルスに攻撃された場合、多数のポータルリダイレクトセッションが開始される可能性があります。このタスクを実行して、そのユーザーに対して確立できるポータルリダイレクトセッションの数を制限できます。

最大数は、HTTPリダイレクトセッションとHTTPSリダイレクトセッションに個別に適用されます。たとえば、最大数を50に設定したとします。これにより、ポータルユーザーは最大100のポータルリダイレクトセッション、50のHTTPリダイレクトセッションおよび50のHTTPSリダイレクトセッションを確立できます。

ワイヤレスネットワークでは、最大数は集中型転送モードでのみ有効です。

手順

1. システムビューに入ります。

   system-view
2. 単一ユーザーのポータルリダイレクトセッションの最大数を設定します。

   portal redirect max-session per-user number

   デフォルトでは、1人のユーザーのポータルリダイレクトセッション数に制限は設定されていません。

APがトラフィック統計情報をACに報告する間隔の設定

このタスクについて

クライアントトラフィック転送ロケーションがAPにある場合、APはトラフィック統計情報を定期的にACにレポートします。

手順

1. システムビューに入ります。

   system-view
2. APがトラフィック統計情報をACに報告する間隔を設定します。

   portal client-traffic-report interval interval

   デフォルトでは、APは60秒ごとにトラフィック統計情報をACに報告します。

ポータルプロトコルパケットからの属性の除外

このタスクについて

ポータルプロトコル属性に対するポータル認証サーバーのサポートは、サーバータイプによって異なります。デバイスが、サーバーでサポートされていない属性を含むパケットをポータル認証サーバーに送信する場合、デバイスとサーバーは通信できません。

この問題に対処するには、ポータル認証サーバーでサポートされていないアトリビュートを伝送しないよう

にポータルプロトコルパケットを設定できます。

ポータル認証サーバーのポータルプロトコルパケットからの属性の除外

1. システムビューに入ります。
   system-view
2. ポータル認証サーバービューに入ります。
   portal server server-name
3. ポータルプロトコルパケットからアトリビュートを除外します。
   exclude-attribute number { ack-auth | ntf-logout | ack-logout }
   デフォルトでは、どのアトリビュートもポータルプロトコルパケットから除外されません。

MACバインディングサーバー用のポータルプロトコルパケットからのアトリビュートの除外

1. システムビューに入ります。
   system-view
2. MACバインディングサーバービューに入ります。
   portal mac-trigger-server server-name
3. ポータルプロトコルパケットからアトリビュートを除外します。
   exclude-attribute attribute-number
   デフォルトでは、どのアトリビュートもポータルプロトコルパケットから除外されません。

サードパーティ認証用のポータル認証のサポートの構成

サードパーティ認証について

このデバイスは、ポータル認証を完了するためのポータル認証サーバーとして、QQ、電子メール、WeChat、またはFacebook認証サーバーなどのサードパーティ認証サーバーの使用をサポートしています。ポータル認証サーバーを配置する必要はなく、ローカルポータルユーザーをデバイス上に作成する必要もありません。これにより、管理および保守のコストが削減されます。

ポータル認証ページにサードパーティ認証ボタンを追加する必要があります。ユーザーがボタンをクリックすると、サードパーティ認証ページにリダイレクトされます。ユーザーはサードパーティ認証アカウントを使用してポータル認証を実行します。

サードパーティ認証の制限事項とガイドライン

ローカルポータルWebサービスを使用する直接ポータル認証のみが、サードパーティ認証をサポートします。

サードパーティ認証用のボタンおよびページの編集

制限事項およびガイドライン

WeChatの認証には認証ボタンも認証ページも必要ありません。

サードパーティ認証ボタンの編集

ポータルユーザーにQQ、電子メール、またはFacebook認証を提供するには、ポータルのログオンページにQQ、電子メール、またはFacebook認証ボタンを追加する必要があります。

QQ認証ボタンを編集する場合は、pt_getQQSubmitUrl()関数を呼び出してQQ認証ページのURLを取得する必要があります。次の例は、QQ認証ボタンのスクリプトの一部を示しています。

```
<html>
<head>
<title>Logon</title>
 <script type="text/javascript" language="javascript" src="pt_private.js"></script>
<script type="text/javascript">
 function setQQUrl(){
 document.getElementById("qqurl").href = pt_getQQSubmitUrl();
 }
</script>
</head>
<body>
... ...
<a href="javascript:void(null)" id="qqurl" onclick="setQQUrl()">QQ</a>
... ...
</body>
</html>
```

電子メールまたはFacebookの認証ボタンを編集するプロセスには、特別な要件はありません。

サードパーティ認証ページの編集

Eメール認証ページとFacebook認証ページを編集する必要があります。QQ認証ページはTencentによって提供されています。

電子メール認証ページを編集する場合は、「認証ページのカスタマイズ」のルールおよび次のルールに従ってください。

- 開始フォームタグのaction属性をmaillogin.htmlに設定します。そうしないと、デバイスはユーザー情報を送信できません。
- ログインページにemailLogon.htmという名前を付けて保存します。

次の例は、emailLogon.htmページのスクリプトの一部を示しています。

```
<form action= maillogin.html method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px" maxlength=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px" maxlength=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;>
</form>
```

Facebook認証ページを編集する場合は、「認証ページのカスタマイズ」の規則に従ってください。

QQ認証の設定

このタスクについて

ポータルユーザーがQQ認証を渡した後、QQ認証サーバーはユーザーの認証コードをポータルWebサ

ーバーに送信します。ポータルWebサーバーは認証コードを受け取った後、ユーザーの認証コード、アプリケーションIDおよびアプリケーションキーをQQ認証サーバーに送信して検証を行います。情報が正しいと検証された場合、デバイスはユーザーがQQ認証を渡したと判断します。

前提条件

ポータルユーザーにQQ認証を提供するには、Tencent Open Platform(http://connect.qq.com/intro/login))にアクセスして以下のタスクを完了する必要があります。
http://connect.qq.com/intro/login)

1. 有効なQQアカウントを使用して開発者として登録します。
2. Webサイトのプラットフォームへのアクセス権を適用します。Webサイトは、QQ認証を通過した後にユーザーがリダイレクトされるWebページです。

アプリケーションが成功すると、Tencent Open PlatformからアプリケーションIDとアプリケーションキーが取得されます。

手順

1. システムビューに入ります。

   system-view
2. QQ認証サーバーを作成し、そのビューに入ります。

   portal extend-auth-server qq
3. (任意)QQ認証サーバーのURLを指定します。

   auth-url url-string

   デフォルトでは、QQ認証サーバーのURLはhttps://graph.qq.comです。
4. (任意)ポータルユーザーがQQ認証を通過した後にリダイレクトされるURLを指定します。

   redirect-url url-string

   デフォルトでは、ポータルユーザーはQQ認証を通過した後にURL http://lvzhou.h3c.com/portal/qqlogin.htmlにリダイレクトされます。
5. (任意)QQ認証用のアプリケーションIDを指定します。

   app-id app-id

   デフォルトでは、QQ認証用のアプリケーションIDが存在します。
6. (任意)QQ認証用のアプリケーションキーを指定します。

   app-key app-key

   デフォルトでは、QQ認証用のappキーが存在します。

電子メール認証の設定

このタスクについて

ポータルユーザーが電子メール認証を選択した場合、ユーザーは電子メール認証を渡した後にネットワークにアクセスできます。

手順

1. システムビューに入ります。

   system-view
2. 電子メール認証サーバーを作成し、そのビューに入ります。

   portal extend-auth-server mail

3. 電子メール認証のプロトコルを指定します。

   mail-protocol { **imap | pop3** } *

   デフォルトでは、電子メール認証用のプロトコルは指定されていません。

4. 電子メール認証用の電子メールドメイン名を指定します。

   mail-domain-name string

   デフォルトでは、電子メール認証用の電子メールドメイン名は指定されていません。

WeChat認証の設定

このタスクについて

WeChat認証中、デバイスはまずWeChat認証のためのクレデンシャル(アプリID、アプリキー、ショップID)をWeChat公式アカウントプラットフォームに送信して検証する。クレデンシャルが検証された後、デバイスはポータル認証を継続し、認証後にユーザーがWiFiネットワークを使用できるようにする。

購読必須機能では、ユーザーはWeChat認証中にWeChat公式アカウントに従う必要があります。ユーザーがWeChat公式アカウントに従わない場合、WeChat認証に失敗します。

登録必須機能が設定されている場合、デバイスはアプリIDとアプリシークレットをWeChat公式アカウント管理プラットフォームに送信してアクセストークンを取得し、ポータルユーザーからの認証要求を受信すると、WeChatサーバーにアクセストークンと認証要求内のオープンIDを送信してユーザー情報を取得する。デバイスは、返されたユーザー情報に基づいて、ポータルユーザーがWeChat公式アカウントに従ったかどうかを判断する。

前提条件

WeChat認証を設定する前に、WeChat Official Account Admin Platform(https://mp.weixin.qq.com)にアクセスして以下のタスクを完了する必要がある。

1. WeChatの公式アカウントを申請する。
2. このアカウントを使ってプラットフォームにログインし、WeChatホットスポット機能を有効にする。
3. デバイス管理タブをクリックし、デバイスを追加します。デバイスが展開されているショップを選択し、ポータルデバイスタイプを選択して、WiFiネットワークのSSIDを入力します。

   上記の設定の後、WeChat認証のためのクレデンシャル(アプリID、アプリキー、ショップID)を取得する。

WeChat認証用のアプリシークレットを取得するには、次のタスクを実行します。

1. WeChat公式アカウントを使用して、WeChat公式アカウント管理プラットフォームにログインする。
2. ナビゲーションツリーから「Developer Centers」を選択します。

   Configuration Items領域にはWeChat Officialアカウントのアプリシークレットが表示される。

手順

1. システムビューに入ります。

   system-view

2. WeChat認証サーバーを作成し、そのビューに入りする。

   portal extend-auth-server wechat

3. (任意)WeChat認証用のアプリIDを指定します。

   app-id app-id

   デフォルトでは、WeChatの認証にアプリIDは指定されていない。

4. (任意)WeChat認証のためのアプリキーを指定します。

   app-key app-key

   デフォルトでは、WeChatの認証にアプリキーは指定されていない。

5. (任意)WeChat認証用のショップIDを指定します。

   shop-id shop-id

   デフォルトでは、WeChatの認証にアプリキーは指定されていない。

6. (任意)加入必須機能を設定します。

   a. 購読必須機能を有効にします。

      subscribe-required enable

      デフォルトでは、subscribe-required機能はディセーブルです。

      この機能は、ポータルの一時パス機能とともに使用する必要があります。一時パス期間を600秒に設定することをお薦めします。

   b. WeChat認証用のアプリシークレットを指定します。

      app-secret { **cipher | simple** } *string*

      デフォルトでは、WeChatの認証にアプリシークレットは指定されていない。

Facebook認証の設定

前提条件

ポータルユーザーに対してFacebook認証を使用するには、FacebookのWebサイトで開発者として登録し、アプリケーションIDとアプリケーションキーを取得する必要があります。

手順

1. システムビューに入ります。

   system-view

2. Facebook認証サーバーを作成し、そのビューに入ります。

   portal extend-auth-server facebook

3. (任意)Facebook認証サーバーのURLを指定します。

   auth-url url-string

   デフォルトでは、Facebook認証サーバーのURLはhttps://graph.facebook.comです。

4. (任意)ポータルユーザーがFacebook認証を通過した後にリダイレクトされるURLを指定します。

   redirect-url url-string

   デフォルトでは、ポータルユーザーはFacebookの認証を通過した後にURL http://oauthindev.h3c.com/portal/fblogin.htmlにリダイレクトされます。
   http://oauthindev.h3c.com/portal/fblogin.html

5. (任意)Facebook認証用のアプリケーションIDを指定します。

   app-id app-id

   デフォルトでは、Facebook認証用のアプリケーションIDは指定されていません。

6. (任意)Facebook認証用のアプリケーションキーを指定します。

   app-key app-key

   デフォルトでは、Facebook認証用のAppキーは指定されていません。

サードパーティ認証用の認証ドメインの指定

このタスクについて

ドメインの認証、認可、およびアカウンティング方式をポータルユーザーに適用するには、インターフェイスまたはサービステンプレートでサードパーティ認証用の認証ドメインを指定します。

制限事項およびガイドライン

指定された認証ドメインの認証、認可、アカウンティングの各方式がnoneであることを確認します。

インターフェイス上のサードパーティ認証用の認証ドメインの指定

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. インターフェイス上のサードパーティ認証用の認証ドメインを指定します。

   portal extend-auth domain domain-name

   デフォルトでは、インターフェイス上のサードパーティ認証に認証ドメインは指定されていません。

サービステンプレートでのサードパーティ認証用の認証ドメインの指定

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. サービステンプレートでサードパーティ認証用の認証ドメインを指定します。

   portal extend-auth domain domain-name

   デフォルトでは、サービステンプレート上のサードパーティ認証に認証ドメインは指定されていません。

サードパーティ認証中にポータルクライアントがアクセスするためのACインターフェイスの指定

このタスクについて

クライアントトラフィックがAPによって転送され、サードパーティポータルの認証が使用されている場合、クライアントはACのIPアドレスを認識できません。クライアントがACに正常にアクセスするには、ACのインターフェイスを指定します。これにより、クライアントはACのIPアドレスを取得してACにアクセスできます。

手順

1. システムビューに入ります。

   system-view
2. サードパーティ認証中にポータルクライアントがアクセスするためのACのインターフェイスを指定します。

   portal client-gateway interface interface-type interface-number

   デフォルトでは、サードパーティ認証中にポータルクライアントがアクセスするためのACインターフェ

イスは指定されていません。

ポータル 一時パスの構成

このタスクについて

通常、ポータルユーザーはポータル認証を渡す前にインターネットにアクセスすることはできません。この機能により、ユーザーがWeChatアカウントを使用してポータル認証を実行した場合、一時的にインターネットにアクセスできます。一時的なパス期間中に、ユーザーはWeChat認証情報をWeChatサーバーに提供し、サーバーがアクセスデバイスと対話してポータル認証を完了できます。

制限事項およびガイドライン

ポータルセーフリダイレクトとポータル一時パスの両方の一致規則が設定されている場合は、ポータル一時パスの一致規則が優先されます。

インターフェイス上のポータル一時パスの構成

1. システムビューに入ります。

   system-view
2. レイヤー3 interfaceビューに入ります。

   interface interface-type interface-number
3. ポータル一時パスをイネーブルにし、インターフェイス上で一時パス期間を設定します。

   portal temp-pass [period period-value] enable

   デフォルトでは、インターフェイス上のポータル一時パスはディセーブルになっています。
4. ポータル一時パスの一致ルールを構成します。
   a. システムビューに戻ります。

      quit
   b. ポータルWebサーバービューに入ります。

      portal web-server server-name
   c. ポータル一時パスの一致ルールを構成します。

      if-match { **original-url** *url-string* | **user-agent** *user-agent* } *
      temp-pass [**redirect-url** *url-string* | original]

      デフォルトでは、ポータル一時パスの一致ルールは設定されていません。

サービステンプレートにポータル一時パスを設定する

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. ポータルの一時パスを有効にし、サービステンプレートに一時パス期間を設定します。

   portal temp-pass [period period-value] enable

   デフォルトでは、ポータルの一時パスはサービステンプレートで無効になっています。
4. ポータル一時パスの一致ルールを構成します。
   a. システムビューに戻ります。

      quit

b. ポータルWebサーバービューに入ります。

portal web-server server-name

c. ポータル一時パスの一致ルールを構成します。

if-match { **original-url** *url-string* | **user-agent** *user-agent* } *
temp-pass [**redirect-url** *url-string* | **original**]

デフォルトでは、ポータル一時パスの一致ルールは設定されていません。

OAuthを使用したポータル認証のユーザー同期間隔の設定

このタスクについて

ポータル認証でOAuthを使用する場合、デバイスはユーザー情報をポータル認証サーバーに定期的にレポートし、サーバー上でユーザーを同期化します。デバイスからポータル認証サーバーへのユーザーの同期化を無効にするには、デバイス上でユーザーの同期化間隔を0秒に設定します。

手順

1. システムビューに入ります。

   system-view

2. OAuthを使用したポータル認証のユーザー同期間隔を設定します。

   portal oauth user-sync interval interval

   デフォルトでは、ユーザー同期間隔は60秒です。

WiFiDogプロトコルを使用したポータル認証用のユーザー同期の構成

このタスクについて

この機能は、ユーザーがWiFiDogプロトコルを使用してポータル認証を実行する場合に使用します。この機能により、デバイスは定期的にユーザー情報をポータルサーバーと同期させ、デバイスとポータルサーバー間のユーザー情報の一貫性を確保できます。

制限事項およびガイドライン

この機能を有効にするには、このタスクを実行する前に、ポータルWebサーバーのタイプがWiFiDogであることを確認してください。ポータルWebサーバーのタイプを指定するには、server-typeコマンドを使用します。

手順

1. システムビューに入ります。

   system-view

2. WiFiDogを使用して、ユーザー情報の同期を有効にし、ポータル認証の同期間隔を設定します。

   portal wifidog user-sync interval interval

   デフォルトでは、WiFiDogを使用したポータル認証ではユーザー情報の同期は無効になっています。

ポータル認証情報レポートの間隔の構成

このタスクについて

この機能を設定した後、デバイスはポータル認証の失敗およびエラー情報をOasisプラットフォームにレポートします。最初のレポートは、デバイスがLvzhouクラウドサーバーに接続されてから30秒後にOasisクラウドサーバーに送信されます。後続のレポートは、この機能で設定されたとおりに定期的に送信されます。

レポート間隔を変更すると、変更された間隔は次のレポートに適用されます。

手順

1. システムビューに入ります。

   system-view
2. ポータル認証情報がOasisプラットフォームに報告される時間間隔を設定します。

   portal cloud report interval minutes

   デフォルトでは、ポータル認証情報は5分間隔でOasisプラットフォームに報告されます。

ポータルロギングの有効化

このタスクについて

セキュリティ監査を容易にするために、ポータルロギングを有効にしてポータル認証情報を記録できます。

ポータルログメッセージを正しく送信するには、デバイスのインフォメーションセンターも構成する必要があります。インフォメーションセンター構成の詳細は、「システム管理構成ガイド」を参照してください。

手順

1. システムビューに入ります。

   system-view
2. ポータルユーザーのログインとログアウトのロギングをイネーブルにします。

   portal user log enable

   デフォルトでは、ポータルユーザーのログインおよびログアウトロギングは使用不可です。
3. ポータルプロトコルパケットのロギングをイネーブルにします。

   portal packet log enable

   デフォルトでは、ポータルプロトコルパケットロギングはディセーブルになっています。
4. ポータルリダイレクトのロギングをイネーブルにします。

   portal redirect log enable

   デフォルトでは、ポータルリダイレクトロギングはディセーブルです。

ポータル認証監視機能の構成

このタスクについて

ポータル認証監視機能では、ポータルユーザーのオフライン、認証失敗および認証エラーが記録されます。これらの記録により、管理者は認証失敗の原因を迅速に特定できます。

手順

1. システムビューに入ります。

   system-view

2. ポータルユーザーのオフライン記録を有効にします。

   portal logout-record enable

   デフォルトでは、ポータルユーザーのオフライン記録は有効になっています。

3. ポータルユーザーのオフラインレコードの最大数を設定します。

   portal logout-record max number

   既定の設定はデバイスモデルによって異なります。詳細については、コマンドリファレンスを参照してください。

4. ポータルユーザーのオフラインレコードをパスにエクスポートします。

   portal logout-record export url *url-string* [start-time start-date start-time end-time end-date end-time]

5. ポータル認証失敗記録をイネーブルにします。

   portal auth-fail-record enable

   デフォルトでは、ポータル認証失敗の記録はイネーブルです。

6. ポータル認証失敗レコードの最大数を設定します。

   portal auth-fail-record max number

   既定の設定はデバイスモデルによって異なります。詳細については、コマンドリファレンスを参照してください。

7. ポータル認証失敗レコードをパスにエクスポートします。

   portal auth-fail-record export url *url-string* [start-time start-date start-time end-time end-date end-time]

8. ポータル認証エラーの記録を有効にします。

   portal auth-error-record enable

   デフォルトでは、ポータル認証エラーの記録はイネーブルです。

9. ポータル認証エラーレコードの最大数を設定します。

   portal auth-error-record max number

   既定の設定はデバイスモデルによって異なります。詳細については、コマンドリファレンスを参照してください。

10. ポータル認証エラーレコードをパスにエクスポートします。

    portal auth-error-record export url *url-string* [*start-time start-date start-time end-time end-date end-time*]

SSIDを切り替えるワイヤレスポータルユーザーのログアウト

このタスクについて

認証されたユーザーが元のサービステンプレートと同じVLANに関連付けられた別のサービステンプレートを介してアクセスするようにSSIDを切り替えると、ユーザーはポータル認証に失敗します。

この機能を使用して、ワイヤレスポータルユーザーがSSIDを切り替えるときに元のサービステンプレートからログアウトし、新しいサービステンプレートでポータル認証を通過できるようにします。

手順

1. システムビューに入ります。

   system-view
2. デバイスがSSIDを切り替えるワイヤレスポータルユーザーをログアウトできるようにします。

   portal user-logoff ssid-switch enable

   デフォルトでは、デバイスはSSIDを切り替えるワイヤレスポータルユーザーをログアウトさせず、ユーザーはオンラインのままです。

ポータルオーセンティケータの中央ACへの切換え

このタスクについて

この作業は、ポータルオーセンティケータがローカルACから中央ACに切り替えられ、転送モードが集中転送からローカル転送に変更されるAC階層で実行します。この作業では、ACを再起動せずにポータルオーセンティケータの切替えを実装できます。

手順

1. システムビューに入ります。

   system-view
2. オーセンティケータをローカルACから中央ACに切り替えます。

   portal authentication-location switchto-central-ac

   ローカルACでこのコマンドを実行します。

ポータルの表示コマンドと保守コマンド

WX1800Hシリーズ、WX2500Hシリーズ、およびWX3000Hシリーズのアクセスコントローラは、IRFモードでのみ使用可能なパラメータやコマンドをサポートしていません。

任意のビューで表示コマンドを実行し、ユーザービューでリセットコマンドを実行します。

タスク	コマンド
ポータル構成とポータルの実行状態を表示します。	**display portal { ap** *ap-name* **[radio** *radio-id* **] | interface** *interface-type interface-number* **}**

タスク	コマンド
ポータル認証サーバーを表示します。	**display portal authentication-location**
ポータル認証エラーレコードを表示します。	**display portal auth-error-record** { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | *start-time start-date start-time end-time end-date end-time* }
ポータル認証失敗レコードを表示します。	**display portal auth-fail-record** { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | *start-time start-date start-time end-time end-date end-time* | **username** *username* }
ポータルキャプティブバイパスのパケット統計情報を表示します。	スタンドアロンモードの場合: **display portal captive-bypass statistics** IRFモードの場合: **display portal captive-bypass statistics** [**slot** *slot-number*]
ポータルユーザーのDHCPリース情報を表示します。	**display [ipv6] portal dhcp-lease [ip** *ip-address* | **ipv6** *ipv6-address*]
宛先ベースのポータルフリー規則のホスト名に対応するIPアドレスを表示します。	**display portal dns free-rule-host [*host-name*]**
サードパーティの認証サーバーに関する情報を表示します。	**display portal extend-auth-server** { **all | facebook | mail | qq | wechat }**
ローカルACからオンラインになったポータルユーザーに関する情報を表示します(このコマンドは中央ACで使用します)。	**display portal local-ac-user { all | ip** *ipv4-address* | **ipv6** *ipv6-address* | **mac** *mac-address* | **local-ac** *local-ac-name* | **username** *username* }
ローカルMACアカウントバインディングエントリに関する情報を表示します。	**display portal local-binding mac-address** { **all** | *mac-address* }
ポータルユーザーのオフラインレコードを表示します。	**display portal logout-record { all | ipv4** *ipv4-address* | **ipv6** *ipv6-address* | *start-time start-date start-time end-time end-date end-time* | **username** *username* }
MACトリガー認証ユーザー(MACトリガー認証を実行するポータルユーザー)に関する情報を表示します。	**display portal mac-trigger user** { **all | ip** *ipv4-address* | **mac** *mac-address* }
MACバインディングサーバーに関する情報を表示します。	**display portal mac-trigger-server** { **all** | **name** *server-name* }

ポータル認証サーバーのパケット統計情報を表示します。	**display portal packet statistics** [**extend-auth-server** { **cloud | facebook | mail | qq | wechat** } | **mac-trigger-server** *server-name* | **server** *server-name*]
ポータル許可ルールの統計情報を表示します。	**display portal permit-rule statistics**
オンラインポータルユーザーのリダイレクトセッション統計情報を表示します。	スタンドアロンモードの場合: **display portal redirect session** [ip *ipv4-address* **| ipv6** *ipv6-address*] IRFモードの場合: **display portal redirect session [ip** *ipv4-address* | **ipv6** *ipv6-address*] [**slot** *slot-number*]
ポータルリダイレクトセッションに関する履歴レコードを表示します。	スタンドアロンモードの場合: **display portal redirect session-record** [*start-time start-date start-time] [end-time end-date end-time*] IRFモードの場合: **display portal redirect session-record** [*start-time start-date start-time] [end-time end-date end-time*] [**slot** *slot-number*]
ポータルリダイレクトセッションに関するサマリー統計情報を表示します。	スタンドアロンモードの場合: **display portal redirect session-statistics** IRFモードの場合: **display portal redirect session-statistics [slot** *slot-number* **]**
ポータルリダイレクトパケットの統計情報を表示します。	スタンドアロンモードの場合: **display portal redirect statistics** IRFモードの場合: **display portal redirect statistics [slot *slot-number*]**
ポータルローミングセンターのパケット統計情報を表示します。	**display portal roaming-center statistics packet**
ポータルルールを表示します。	スタンドアロンモードの場合: **display portal rule** { **all | dynamic | static } { ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* } IRFモードの場合: **display portal rule** { **all | dynamic | static } { ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-numbe*r [**slot** *slot-number*] }

ポータルセーフリダイレクトのパケット統計情報を表示します。	スタンドアロンモードの場合: **display portal safe-redirect statistics** IRFモードの場合: **display portal safe-redirect statistics** [**slot** *slot-number*]
ポータル認証サーバー情報を表示します。	**display portal server** [server-name]
ポータルユーザー情報を表示します。	**display portal user { all | ap ap-name** [**radio** *radio-id*] | **auth-type { cloud | email | facebook | local | mac-trigger | normal | qq | wechat } | interface** *interface-type interface-number* | **ip** *ip-address* | **ipv6** *ipv6-address* | **mac mac-address | pre-auth [interface** *interface-type interface-number* | **ip** *ip-address* | **ipv6** *ipv6-address*] | **username** *username* } **[brief | verbose**]
ポータルユーザー数を表示します。	**display portal user count**
ポータルWebサーバー情報を表示します。	**display portal web-server [server-name]**
Webリダイレクト規則情報を表示します。	スタンドアロンモードの場合: **display web-redirect rule { ap** *ap-name* [**radio** *radio-id*] | **interface** i*nterface-type interface-number* } IRFモードの場合: **display web-redirect rule { ap ap-name** [**radio** *radio-id*] | **interface** *interface-type interface-number* [**slot** *slot-number*] }
ポータル認証エラーレコードを消去します。	**reset portal auth-error-record { all | ipv4** *ipv4-address* | **ipv6** *ipv6-address* | *start-time start-date start-time end-time end-date end-time* }
ポータル認証失敗レコードを消去します。	**reset portal auth-fail-record { all | ipv4** *ipv4-address* | **ipv6** *ipv6-address* | *start-time start-date start-time end-time end-date end-time* | **username** *username* }
ポータルキャプティブバイパスのパケット統計情報をクリアします。	スタンドアロンモードの場合: **reset portal captive-bypass statistics** IRFモードの場合: **reset portal captive-bypass statistics** [**slot** *slot-number*]
ローカルMACアカウントバインディングエントリをクリアします。	**reset portal local-binding mac-address** { *mac-address* | **all** }

ポータルユーザーのオフラインレコードを消去します。	**reset portal logout-record { all | ipv4** *ipv4-address* | **ipv6** *ipv6-address* | *start-time start-date start-time end-time end-date end-time* | **username** *username* }
ポータル認証サーバーのパケット統計情報をクリアします。	**reset portal packet statistics** [**extend-auth-server** { **cloud** | **facebook** | **mail** | **qq** | **wechat** } | **mac-trigger-server** *server-name* | **server** *server-name*]
ポータルリダイレクトセッションに関する履歴レコードを消去します。	スタンドアロンモードの場合: **reset portal redirect session-record** IRFモードの場合: **reset portal redirect session-record** **[slot *slot-number*]**
ポータルリダイレクトセッションのサマリー統計情報をクリアします。	スタンドアロンモードの場合: **reset portal redirect session-statistics** IRFモードの場合: **reset portal redirect** **session-statistics** [**slot** *slot-number*]
ポータルリダイレクトパケット統計情報をクリアします。	スタンドアロンモードの場合: **reset portal redirect statistics** IRFモードの場合: **reset portal redirect statistics** [**slot** *slot-number*]
ポータルローミングセンターのパケット統計情報をクリアします。	**reset portal roaming-center statistics packet**
ポータルセーフリダイレクトのパケット統計情報をクリアします。	スタンドアロンモードの場合: **reset portal safe-redirect statistics** IRFモードの場合: **reset portal safe-redirect statistics** [**slot** *slot-number*]

ポータル構成の例

このドキュメントのAPモデルとシリアル番号は、例としてのみ使用されています。APモデルとシリアル番号のサポートは、ACモデルによって異なります。

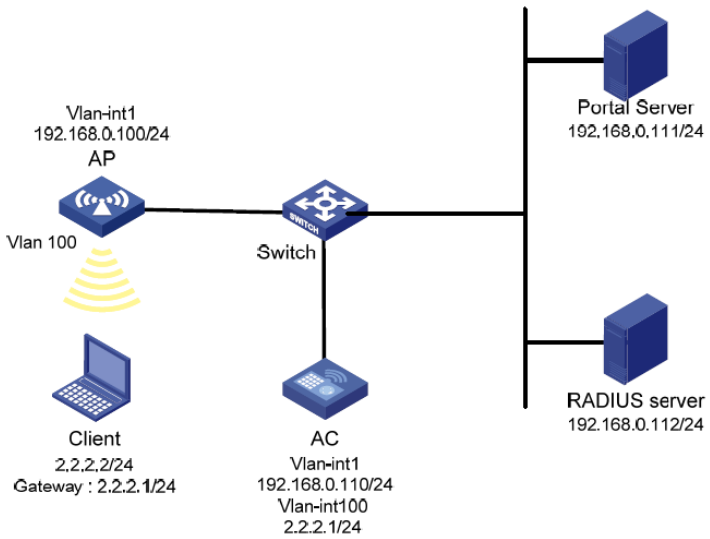
例:VLANインターフェイスでの直接ポータル認証の設定

ネットワーク構成

図6に示すように、APはクライアントからのユーザートラフィックを直接転送します。クライアントには、手動またはDHCPを介してパブリックIPアドレスが割り当てられます。iMCサーバーは、ポータル認証サーバーおよびポータルWebサーバーの両方として機能します。RADIUSサーバーは、認証/会計サーバーとして機能します。この例では、iMCサーバーはiMC PLAT7.1(E0303)およびiMC UAM7.1(E0304)を実行します。

クライアントが認証を渡す前にポータルWebサーバーのみにアクセスし、認証を渡した後に他のネットワークリソースにアクセスできるように、直接ポータル認証を構成します。

図6 ネットワーク図



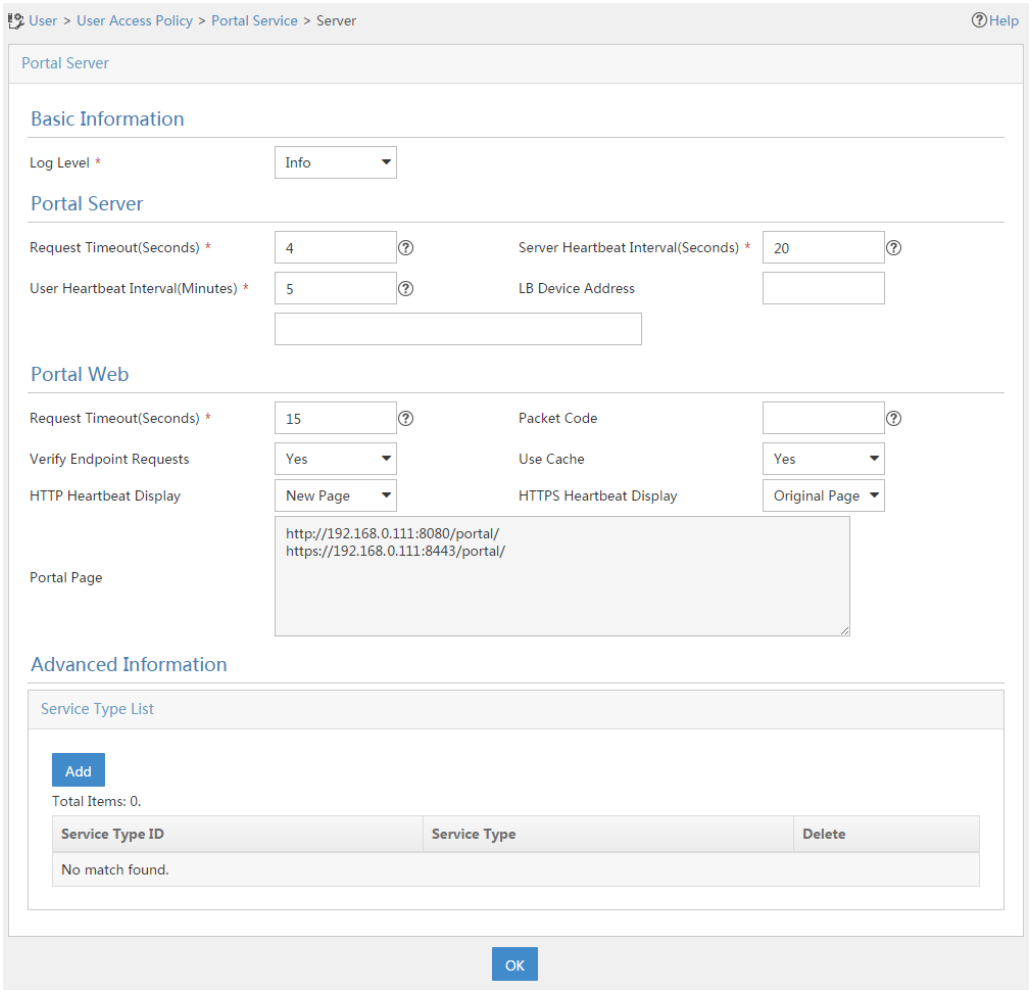
RADIUSサーバーの設定

#認証およびアカウンティング機能を提供するようにRADIUSサーバーを正しく設定します(詳細は省略します)。

ポータルサーバーの構成

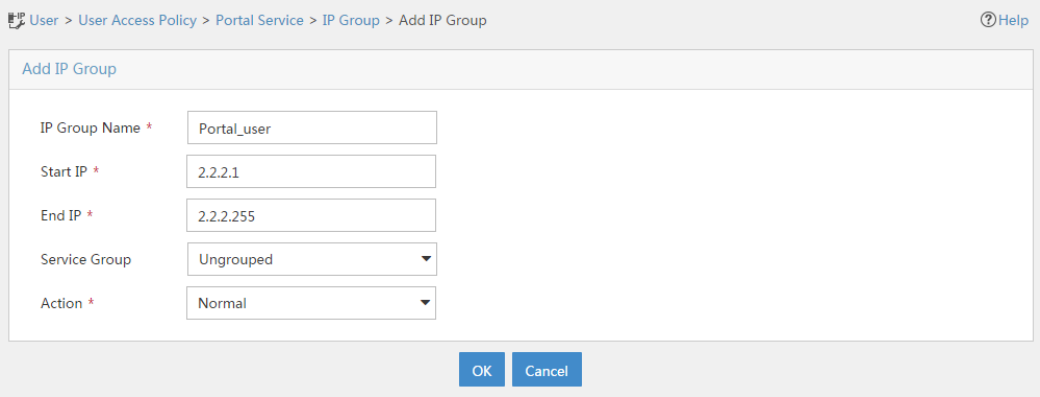
1. ポータルサーバーを構成します。
   a. iMCにログインして、Userタブをクリックします。
   b. 図7に示すように、ナビゲーションツリーからUser Access Policy > Portal Service > Serverを選択して、ポータルサーバーの構成ページを開きます。
   c. 必要に応じてポータルサーバーパラメータを構成します。この例では、デフォルト設定を使用しています。
   d. OKをクリックします。

図7 ポータルサーバーの構成



2. 次のようにIPアドレスグループを設定します。
   a. ナビゲーションツリーからUser Access Policy > Portal Service > IP Groupを選択して、ポータルIPアドレスグループの設定ページを開きます。
   b. 図8に示すように、Addをクリックしてページを開きます。
   c. IPグループ名を入力します。
   d. IPグループの開始IPアドレスと終了IPアドレスを入力します。ホストIPアドレスがIPグループに含まれていることを確認してください。
   e. サービスグループを選択します。
      この例では、既定のグループUngroupedを使用します。
   f. アクションNormalを選択します。
   g. OKをクリックします。

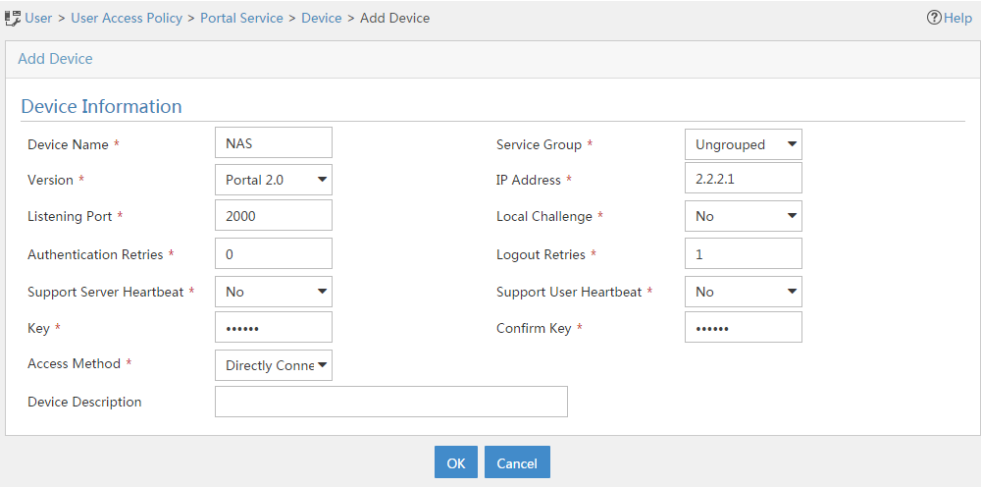
図8 IPアドレスグループの追加



3. ポータルデバイスを追加します。
   a. ナビゲーションツリーからUser Access Policy > Portal Service > Deviceを選択して、ポータルデバイスの設定ページを開きます。
   b. 図9に示すように、Addをクリックしてページを開きます。
   c. デバイス名NASを入力します。
   d. ポータルサーバーと情報を交換するACのインターフェイスのIPアドレスを入力します。
   e. サーバーハートビートおよびユーザーハートビート機能をサポートするかどうかを選択します。

      この例では、Support Server HeartbeatとSupport User Heartbeatの両方に対してNoを選択します。
   f. キーを入力します。キーは、ACに設定されているキーと同じである必要があります。
   g. Access MethodリストからAccess Methodを選択します。
   h. OKをクリックします。

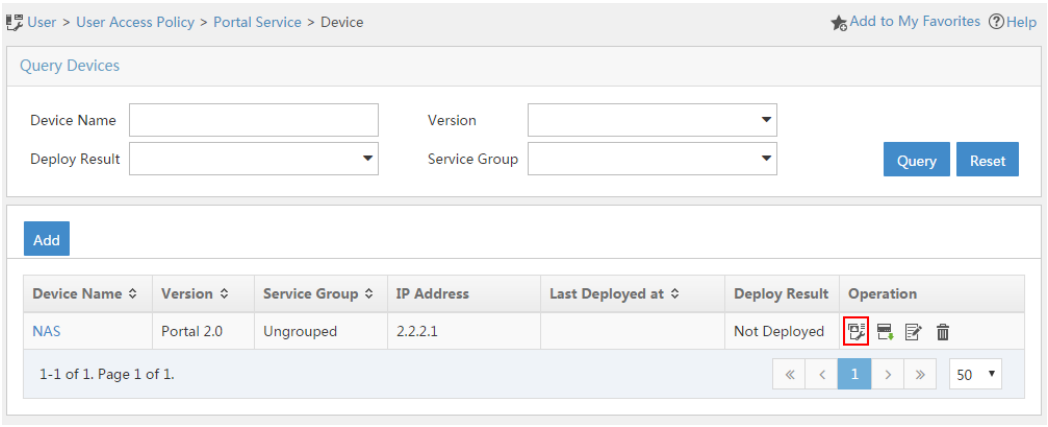
図9 ポータルデバイスの追加



4. ポータルデバイスをIPアドレスグループに関連付けます。
   a. 図10に示すように、Port Group Information Managementをクリックします。デバイスのコイン

      NAS: ポートグループの構成ページを開きます。

図10 デバイスリスト



b. 図11に示すように、Addをクリックしてページを開きます。

c. ポートグループ名を入力します。

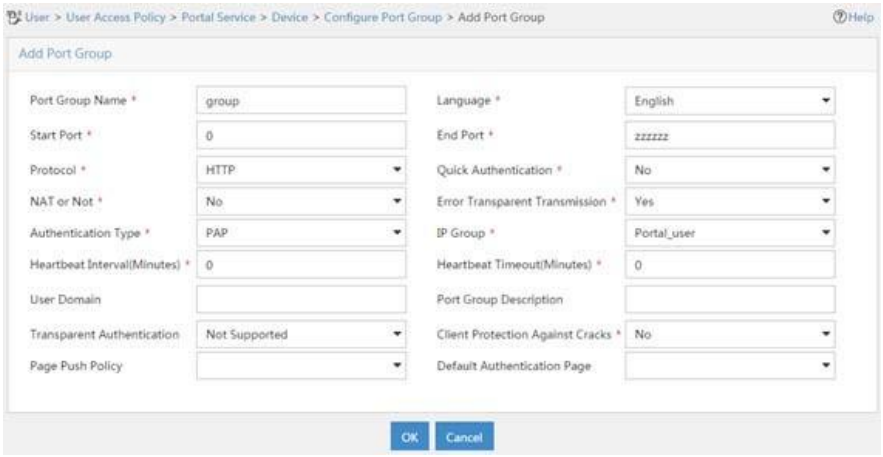
d. 設定済みのIPアドレスグループを選択します。

ユーザーがネットワークにアクセスするために使用するIPアドレスは、このIPアドレスグループ内にある必要があります。

e. その他のパラメータにはデフォルト設定を使用します。

f. OKをクリックします。

図11 ポートグループの追加



ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できることを確認します(詳細は示されていません)。

2. RADIUSスキームを設定します。

#rs1という名前のRADIUSスキームを作成し、そのビューに入ります。

<AC> system-view

[AC] radius scheme rs1

#プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと

通信するためのキーを設定します。

[AC-radius-rs1] primary authentication 192.168.0.112

[AC-radius-rs1] primary accounting 192.168.0.112

[AC-radius-rs1] key authentication simple radius

[AC-radius-rs1] key accounting simple radius

#RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

[AC-radius-rs1] user-name-format without-domain

[AC-radius-rs1] quit

#RADIUSセッション制御をイネーブルにします。

[AC] radius session-control enable

3. 認証ドメインを構成します。

#dm1という名前のISPドメインを作成し、そのビューに入ります。

[AC] domain dm1

#ISPドメインのAAA方式を設定します。

[AC-isp-dm1] authentication portal radius-scheme rs1

[AC-isp-dm1] authorization portal radius-scheme rs1

[AC-isp-dm1] accounting portal radius-scheme rs1

[AC-isp-dm1] quit

#ドメインdm1をデフォルトのISPドメインとして構成します。ユーザーがログイン時にISPドメイン名なしでユーザー名を入力した場合、デフォルトドメインの認証および会計方法がユーザーに使用されます。

[AC] domain default enable dm1

4. ポータル認証を構成します。

#ポータル認証サーバーを構成します。

[AC] portal server newpt

[AC-portal-server-newpt] ip 192.168.0.111 key simple portal

[AC-portal-server-newpt] port 50100

[AC-portal-server-newpt] quit

ポータルWebサーバーの設定をします。

[AC] portal web-server newpt

[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

[AC-portal-websvr-newpt] quit

#VLANインターフェイス100上で直接ポータル認証をイネーブルにします。

[AC] interface vlan-interface 100

[AC–Vlan-interface100] portal enable method direct

VLAN-interface 100上でポータルWebサーバー newpt を指定します

[AC–Vlan-interface100] portal apply web-server newpt

#ACからポータル認証サーバーに送信されるポータルパケットのBAS-IPを2.2.2.1に設定します。

[AC–Vlan-interface100] portal bas-ip 2.2.2.1

[AC–Vlan-interface100] quit

設定の確認

#ポータル構成が有効になっていることを確認します。

[AC] display portal interface vlan-interface 100 Portal

information of Vlan-interface100

NAS-ID profile: Not configured

VSRP instance : Not

configured VSRP state: N/A

Authorization : Strict checking

ACL: Disabled

User profile : Disabled

Dual stack : Disabled

Dual traffic-separate: Disabled

IPv4:

Portal status:

Enabled VSRP_SM

state: M_Delay

Portal authentication method: Direct Portal

Web server: newpt(active)

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

Pre-auth domain: Not

configured User-dhcp-only:

Disabled

Pre-auth IP pool: Not configured

Max portal users: Not

configured Bas-ip: 2.2.2.1

User Detection: Not

configured Action for server

detection:

Server type Server nameAction

Layer3 source network:

IP addressMask

Destination authenticate subnet:

IP addressMask

IPv6:

Portal status: Disabled

VSRP_SM state:

M_Delay

Portal authentication method: Disabled

Portal Web server: Not configured

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

Pre-auth domain: Not

configured User-dhcp-only:

Disabled

Pre-auth IP pool: Not configured

Max portal users: Not

configured Bas-ipv6: Not

configured

User detection: Not

configured Action for server

detection:

Server type Server nameAction

Layer3 source network:

IP addressPrefix length

Destination authenticate subnet:

IP addressPrefix length

ユーザーは、H3C iNodeクライアントまたはWebブラウザを使用してポータル認証を実行できます。passingtheauthenticationの前にtheusercanaccessonlytheauthenticationpage

http://192.168.0.111:8080/portalユーザーからのすべてのWeb要求は、認証ページにリダイレクトされます。ユーザーは認証を受けた後、他のネットワークリソースにアクセスできます。

#ユーザーが認証にパスした後、ポータルユーザーに関する情報を表示します。

[AC] display portal user interface vlan-interface 100 Total

portal users: 1

Username: abc

Portal server:

newpt State:

Online

VPN instance: N/A

MACIPVLANInterface

0015-e9a6-7cfe2.2.2.2100Vlan-interface100 Authorization

information:

DHCP IP pool:

N/A User

profile: N/A

Session group profile:

N/A ACL: N/A

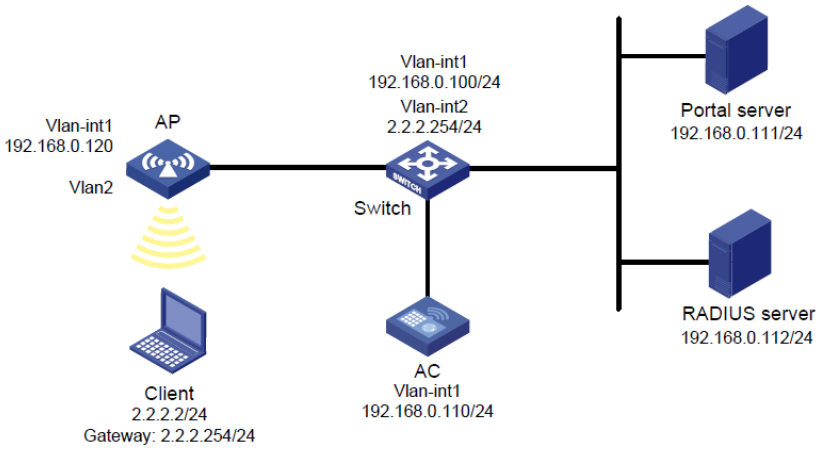
例:サービステンプレートでの直接ポータル認証の設定

ネットワーク構成

図12に示すように、APはクライアントからのユーザートラフィックを直接転送します。クライアントには、手動またはDHCPを介してパブリックIPアドレスが割り当てられます。ポータルサーバーは、ポータル認証サーバーとポータルWebサーバーの両方として機能します。RADIUSサーバーは、認証/会計サーバーとして機能します。

クライアントが認証を渡す前にポータルWebサーバーのみにアクセスし、認証を渡した後に他のネットワークリソースにアクセスできるように、直接ポータル認証を構成します。

図12 ネットワーク図



RADIUSサーバーの設定

認証およびアカウンティング機能を提供するようにRADIUSサーバーを正しく設定します(詳細は表示されません)。

ポータルサーバーの構成

ポータルサーバーの構成の詳細は、「例:VLANインターフェイスでの直接ポータル認証の構成」を参照してください。

APの設定

APがACと通信できるようにAPを設定します(詳細は省略します)。

ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達で

きることを確認します(詳細は省略します)。

2. RADIUSスキームを設定します。

   #rs1という名前のRADIUSスキームを作成し、そのビューに入ります。

   <AC> system-view

   [AC] radius scheme rs1

   #プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

   [AC-radius-rs1] primary authentication 192.168.0.112

   [AC-radius-rs1] primary accounting 192.168.0.112

   [AC-radius-rs1] key authentication simple radius

   [AC-radius-rs1] key accounting simple radius

   #RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

   [AC-radius-rs1] user-name-format without-domain

   [AC-radius-rs1] quit

   #RADIUSセッション制御をイネーブルにします。

   [AC] radius session-control enable

3. 認証ドメインを構成します。

   #dm1という名前のISPドメインを作成し、そのビューに入りします。

   [AC] domain dm1

   #ISPドメインのAAA方式を設定します。

   [AC-isp-dm1] authentication portal radius-scheme rs1

   [AC-isp-dm1] authorization portal radius-scheme rs1

   [AC-isp-dm1] accounting portal radius-scheme rs1

   [AC-isp-dm1] quit

   #ドメインdm1をデフォルトのISPドメインとして構成します。ユーザーがログイン時にISPドメイン名なしでユーザー名を入力した場合、デフォルトドメインの認証および会計方法がユーザーに使用されます。

   [AC] domain default enable dm1

4. ポータル認証を構成します。

   #ポータル認証サーバーを設定します。

   [AC] portal server newpt

   [AC-portal-server-newpt] ip 192.168.0.111 key simple portal

   [AC-portal-server-newpt] port 50100

   [AC-portal-server-newpt] quit

   # ポータルWebサーバーを設定します。

   [AC] portal web-server newpt

[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

[AC-portal-websvr-newpt] quit

#手動AP ap2を作成し、APモデルとシリアルIDを指定します。

[AC] wlan ap ap2 model WA4320i-ACN

[AC-wlan-ap-ap2] serial-id 210235A29G007C000020

#サービステンプレートnewstを作成し、SSIDをportal1に設定します。

[AC] wlan service-template newst

[AC–wlan-st-newst] ssid portal_1

#サービステンプレートnewstで直接認証をイネーブルにします。

[AC–wlan-st-newst] portal enable method direct

#サービステンプレートnewstのポータルWebサーバーnewptを指定します。

[AC–wlan-st-newst] portal apply web-server newpt

#ACからポータル認証サーバーに送信されるポータルパケットのBAS-IPを192.168.0.110に設定します。

[AC–wlan-st-newst] portal bas-ip 192.168.0.110

Configure the AP to forward client data traffic.

[AC–wlan-st-newst] client forwarding-location ap

サービステンプレート newstを有効にします。

[AC–wlan-st-newst] service-template enable

[AC–wlan-st-newst] quit

#APの無線2の作業チャネルをチャネル11に設定します。

[AC] wlan ap ap2

[AC-wlan-ap-ap2] radio 2

[AC-wlan-ap-ap2-radio-2] channel 11

#radio2をイネーブルにし、サービステンプレートnewstおよびVLAN2をradio2にバインドします。

[AC-wlan-ap-ap2-radio-2] radio enable

[AC-wlan-ap-ap2-radio-2] service-template newst vlan 2

[AC-wlan-ap-ap2-radio-2] quit

[AC-wlan-ap-ap2] quit

設定の確認

#ポータル構成が有効になっていることを確認します。

[AC] display portal ap ap2

Portal information of ap2

Radio ID: 2

SSID: portal_1

Authorization : Strict checking

ACL: Disable

User profile : Disable

Dual stack: Disabled

Dual traffic-separate: Disabled

IPv4:

Portal status:

Enabled VSRP_SM

state: M_Delay

Portal authentication method: Direct Portal

Web server: newpt(active)

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

User-dhcp-only: Disabled

Max portal users: Not configured

Bas-ip: 192.168.0.110

Action for server detection:

Server typeServer nameAction

Destination authentication subnet:

IP addressMask

IPv6:

Portal status: Disabled

VSRP_SM state:

M_Delay

Portal authentication method: Disabled

Portal Web server: Not configured

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

User-dhcp-only: Disabled

Max portal users: Not

configured Bas-ipv6: Not

configured

Action for server detection:

Server typeServer nameAction

Destination authentication subnet:

IP addressPrefix length

ユーザーは、H3C iNodeクライアントまたはWebブラウザを使用してポータル認証を実行できます。認証を渡す前にアクセスできるのは、認証ページhttp://192.168.0.111:8080/portalのみです。ユーザーからのすべてのWeb要求は、認証ページにリダイレクトされます。認証を渡した後、ユーザーは他のネットワークリソースにアクセスできます。

#ユーザーが認証にパスした後、ポータルユーザーに関する情報を表示します。

[AC] display portal user ap ap2

Total portal users: 1

Username: 1

AP name:

ap2 Radio

ID: 2 SSID:

portal_1

Portal server:

newpt State:

Online

VPN instance: N/A

MACIPVLANInterface

0015-005e-9398 2.2.2.22WLAN-BSS1/0/1

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile:

N/A ACL number: N/A

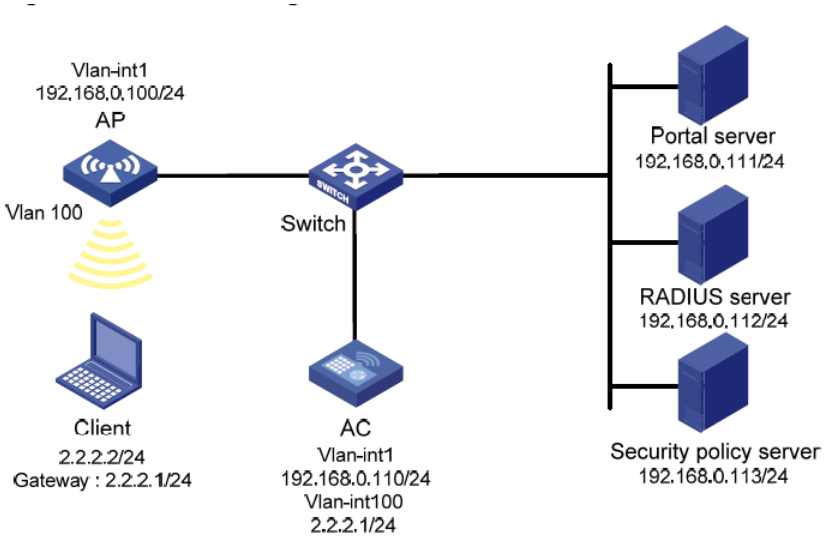
例:拡張直接ポータル認証の設定

ネットワーク構成

図13に示すように、クライアントはAPを介してACに接続されています。クライアントには、パブリックIPアドレスが手動またはDHCPを介して割り当てられています。ポータルサーバーは、ポータル認証サーバーとポータルWebサーバーの両方として機能します。RADIUSサーバーは、認証/会計サーバーとして機能します。

拡張直接ポータル認証を構成します。アイデンティティ認証を渡した後でクライアントがセキュリティチェックに失敗した場合、クライアントはサブネット192.168.0.0/24にのみアクセスできます。セキュリティチェックにパスした後、クライアントは他のネットワークリソースにアクセスできます。

図13 ネットワーク図



RADIUSサーバーおよびポータルサーバーの設定

#RADIUSサーバーおよびポータルサーバーを正しく設定して、認証およびアカウンティング機能を提供します(詳細は省略します)。

ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できることを確認します(詳細は省略します)。
2. RADIUSスキームを設定します。

   #rs1という名前のRADIUSスキームを作成し、そのビューに入ります。

   <AC> system-view

   [AC] radius scheme rs1

   #プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

   [AC-radius-rs1] primary authentication 192.168.0.112

   [AC-radius-rs1] primary accounting 192.168.0.112

   [AC-radius-rs1] key accounting simple radius

   [AC-radius-rs1] key authentication simple radius

   #RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

   [AC-radius-rs1] user-name-format without-domain

   #IPアドレスが192.168.0.113のセキュリティポリシーサーバーを指定します。

   [AC-radius-rs1] security-policy-server 192.168.0.113

   [AC-radius-rs1] quit

   #RADIUSセッション制御をイネーブルにします。

   [AC] radius session-control enable

   #IPアドレスが192.168.0.112で共有キーが12345のセッション制御クライアントをプレーンテキスト形式で指定します。

[AC] radius session-control client ip 192.168.0.112 key simple 12345

3. 認証ドメインを構成します。

   #dm1という名前のISPドメインを作成し、そのビューに入ります。

   [AC] domain dm1

   #ISPドメインのAAA方式を設定します。

   [AC-isp-dm1] authentication portal radius-scheme rs1

   [AC-isp-dm1] authorization portal radius-scheme rs1

   [AC-isp-dm1] accounting portal radius-scheme rs1

   [AC-isp-dm1] quit

   #ドメインdm1をデフォルトのISPドメインとして構成します。ユーザーがログイン時にISPドメイン名なしでユーザー名を入力した場合、デフォルトドメインの認証および会計方法がユーザーに使用されます。

   [AC] domain default enable dm1

4. ACL3000を分離ACLとして設定し、ACL3001をセキュリティACLとして設定します。

   [AC] acl advanced 3000

   [AC-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255

   [AC-acl-ipv4-adv-3000] rule deny ip

   [AC-acl-ipv4-adv-3000] quit

   [AC] acl advanced 3001

   [AC-acl-ipv4-adv-3001] rule permit ip

   [AC-acl-ipv4-adv-3001] quit

注:

セキュリティーポリシーサーバー上で、ACL3000を分離ACLとして指定し、ACL3001をセキュリティーACLとして指定していることを確認してください。

5. ポータル認証を構成します。

   #ポータル認証サーバーを設定します。

   [AC] portal server newpt

   [AC-portal-server-newpt] ip 192.168.0.111 key simple portal

   [AC-portal-server-newpt] port 50100

   [AC-portal-server-newpt] quit

   # ポータルWebサーバーを設定します。

   [AC] portal web-server newpt

   [AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

[AC-portal-websvr-newpt] quit

#VLANインターフェイス100上で直接ポータル認証をイネーブルにします。

[AC] interface vlan-interface 100

[AC–Vlan-interface100] portal enable method direct

VLAN-interface 100上にポータルWebサーバーnewptを設定します。

[AC–Vlan-interface100] portal apply web-server newpt

#VLANインターフェイス100からポータル認証サーバーに送信されるポータルパケットのBAS-IPを2.2.2.1に設定します。

[AC–Vlan-interface100] portal bas-ip 2.2.2.1

[AC–Vlan-interface100] quit

設定の確認

#ポータル構成が有効になっていることを確認します。

[AC] display portal interface vlan-interface 100 Portal

information of Vlan-interface100

NAS-ID profile: Not configured

VSRP instance : Not

configured VSRP state: N/A

Authorization : Strict checking

ACL: Disabled

User profile : Disabled

Dual stack: Disabled

Dual traffic-separate: Disabled

IPv4:

Portal status: Enabled

Portal authentication method: Direct Portal

Web server: newpt(active)

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

Pre-auth domain: Not

configured User-dhcp-only:

Disabled

Pre-auth IP pool: Not configured

Max portal users: Not

configured Bas-ip: 2.2.2.1

User Detection: Not

configured Action for server

detection:

Server type Server nameAction

Layer3 source network:

IP addressMask

Destination authenticate subnet:

IP addressMask

IPv6:

Portal status: Disabled

Portal authentication method: Disabled

Portal Web server: Not configured

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

Pre-auth domain: Not

configured User-dhcp-only:

Disabled

Pre-auth IP pool: Not configured

Max portal users: Not

configured Bas-ipv6: Not

configured

User detection: Not

configured Action for server

detection:

Server typeServer nameAction

Layer3 source network:

IP addressPrefix length

Destination authenticate subnet:

IP addressPrefix length

ポータル認証を渡す前に、H3C iNodeクライアントを使用するユーザーは認証ページ http://192.168.0.111:8080/portalにのみアクセスできます。ユーザーからのすべてのWeb要求は認証ページにリダイレクトされます。

- ユーザーは、ID認証だけを渡した後、ACL3000によって許可されたリソースにアクセスできます。
- ユーザーは、ID認証とセキュリティチェックの両方を通過した後、ACL3001によって許可されたネットワークリソースにアクセスできます。

#ユーザーがID認証とセキュリティチェックに合格したら、ポータルユーザーに関する情報を表示し

ます。

```
[AC] display portal user interface vlan-interface 100 Total
portal users: 1
Username: abc
  Portal server:
  newpt State:
  Online
  VPN instance: N/A

  MAC             IP              VLAN  Interface
  0015-e9a6-7cfe  2.2.2.2         --    Vlan-interface100
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile:
    N/A ACL: 3001
```

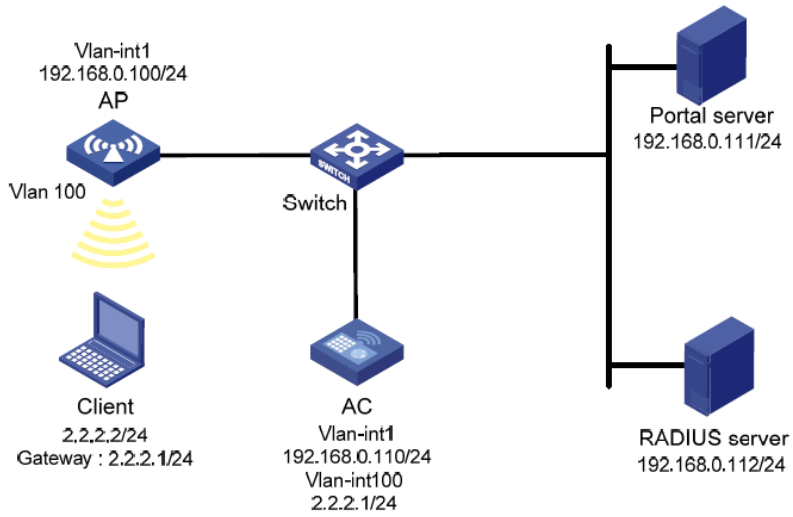
例:ポータルサーバーの検出の構成

ネットワーク構成

図14に示すように、クライアントはAPを介してACに接続されています。クライアントには、パブリックIPアドレスが手動またはDHCPを介して割り当てられています。iMCサーバーは、ポータル認証サーバーおよびポータルWebサーバーの両方として機能します。RADIUSサーバーは、認証/会計サーバーとして機能します。この例では、iMCサーバーはiMC PLAT7.1(E0303)およびiMC UAM7.1(E0304)を実行します。

- クライアントが認証を渡す前にポータルサーバーのみにアクセスし、認証を渡した後に他のネットワークリソースにアクセスできるように、ACで直接ポータル認証を構成します。
- ポータル認証サーバーの到達可能性ステートを検出し、ステートの変更時にログメッセージを送信し、認証サーバーが到達不能な場合にポータル認証をディセーブルにするようにACを設定します。

図14 ネットワーク図



RADIUSサーバーの設定

#認証およびアカウンティング機能を提供するようにRADIUSサーバーを正しく設定します(詳細は省略します)。

ポータルサーバーの構成

1. ポータルサーバーを構成します。

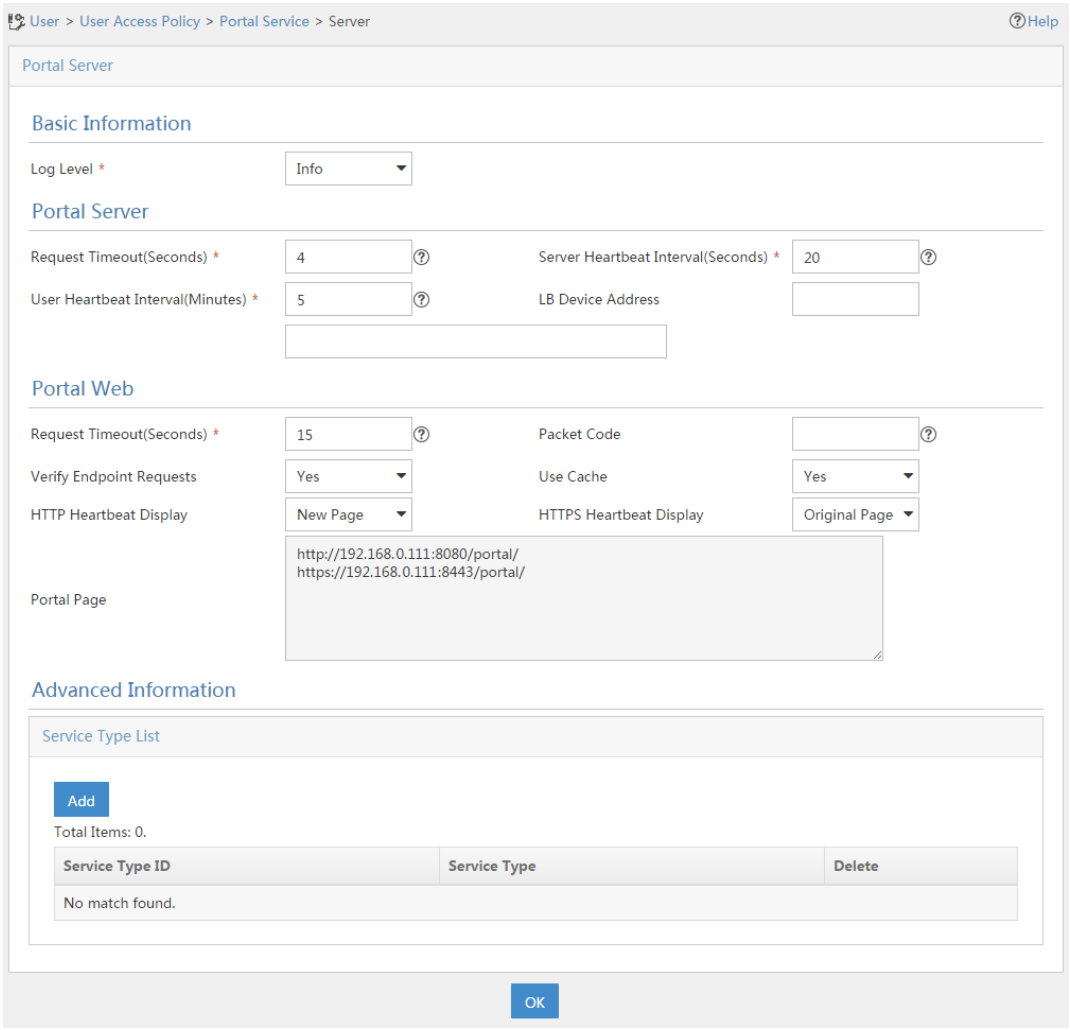
iMCにログインして、Userタブをクリックします。

a. 図15に示すように、ナビゲーションツリーからUser Access Policy > Portal Service > Serverを選択して、ポータルサーバーの構成ページを開きます。

b. 必要に応じてポータルサーバーパラメータを構成します。この例では、デフォルト設定を使用しています。

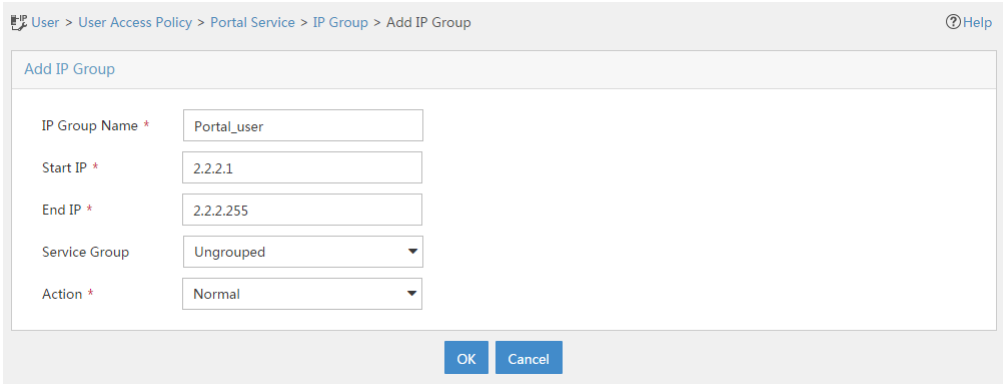
c. OKをクリックします。

図15 ポータル認証サーバーの構成



2. 次のようにIPアドレスグループを設定します。
   a. ナビゲーションツリーからUser Access Policy > Portal Service > IP Groupを選択して、ポータルIPアドレスグループの設定ページを開きます。
   b. 図16に示すように、Addをクリックしてページを開きます。
   c. IPグループ名を入力します。
   d. IPグループの開始IPアドレスと終了IPアドレスを入力します。ホストIPアドレスがIPグループに含まれていることを確認してください。
   e. サービスグループを選択します。
      この例では、既定のグループUngroupedを使用します。
   f. ActionリストからNormalを選択します。
   g. OKをクリックします。

図16 IPアドレスグループの追加



3. ポータルデバイスを追加します。

   a. ナビゲーションツリーからUser Access Policy > Portal Service > Deviceを選択して、ポータルデバイスの設定ページを開きます。

   b. 図17に示すように、Addをクリックしてページを開きます。

   c. デバイス名NASを入力します。

   d. ホストに接続されているACのインターフェイスのIPアドレスを入力します。

   e. サーバーハートビートおよびユーザーハートビート機能をサポートするかどうかを選択します。

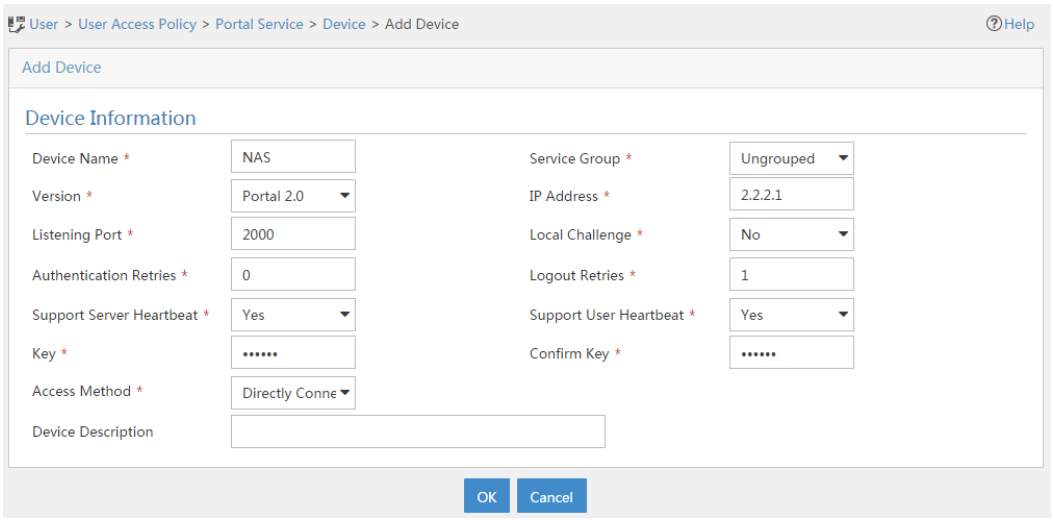
      この例では、Support Server HeartbeatとSupport User Heartbeatの両方に対してYesを選択します。

   f. キーを入力します。キーは、ACに設定されているキーと同じである必要があります。

   g. Access MethodリストからDireclty Connectedを選択します。

   h. OKをクリックします。

図17 ポータルデバイスの追加

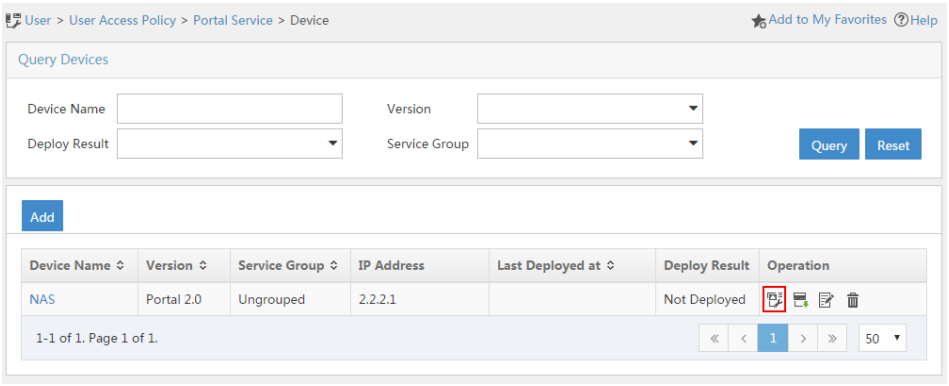


4. ポータルデバイスをIPアドレスグループに関連付けます。

   a. 図18に示すように、デバイスのPort Group Information Managementアイコンをクリックします。

      NAS: ポートグループの構成ページを開きます。

図18 デバイスリスト



b. 図19に示すように、Addをクリックしてページを開きます。

c. ポートグループ名を入力します。

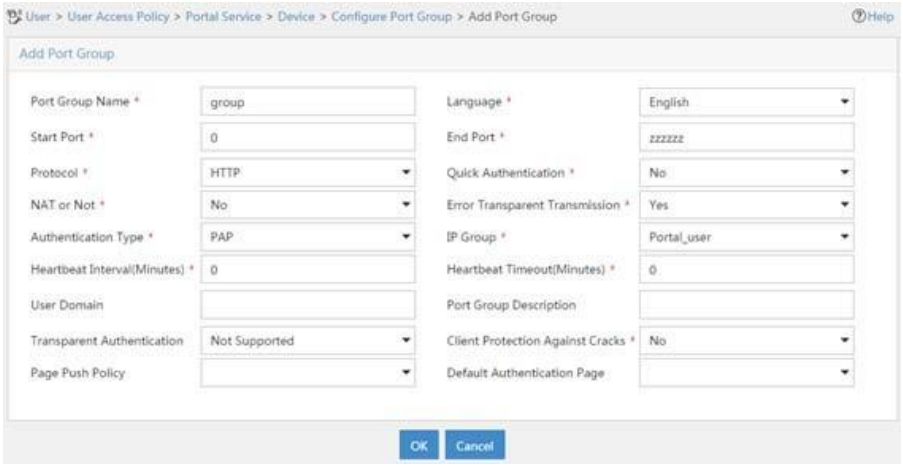
d. 設定済みのIPアドレスグループを選択します。

ユーザーがネットワークにアクセスするために使用するIPアドレスは、このIPアドレスグループ内にある必要があります。

e. その他のパラメータにはデフォルト設定を使用します。

f. OKをクリックします。

図19 ポートグループの追加



ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できることを確認します(詳細は省略します)。

2. RADIUSスキームを設定します。

#rs1という名前のRADIUSスキームを作成し、そのビューに入ります。

<AC> system-view

[AC] radius scheme rs1

#プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

[AC-radius-rs1] primary authentication 192.168.0.112

[AC-radius-rs1] primary accounting 192.168.0.112

[AC-radius-rs1] key authentication simple radius

[AC-radius-rs1] key accounting simple radius

RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

[AC-radius-rs1] user-name-format without-domain

[AC-radius-rs1] quit

RADIUSセッション制御をイネーブルにします。

[AC] radius session-control enable

3. 認証ドメインを設定します。

dm1という名前のISPドメインを作成し、そのビューに入ります。

[AC] radius session-control enable

ISPドメインのAAA方式を設定します。

[AC-isp-dm1] authentication portal radius-scheme rs1

[AC-isp-dm1] authorization portal radius-scheme rs1

[AC-isp-dm1] accounting portal radius-scheme rs1

[AC-isp-dm1] quit

ドメインdm1をデフォルトのISPドメインとして構成します。ユーザーがログイン時にISPドメイン名なしでユーザー名を入力した場合、デフォルトドメインの認証および会計方法がユーザーに使用されます。

[AC] domain default enable dm1

4. ポータル認証を設定します。

ポータル認証サーバーを設定します。

[AC] portal server newpt

[AC-portal-server-newpt] ip 192.168.0.111 key simple portal

[AC-portal-server-newpt] port 50100

#ポータル認証サーバーの到達可能性検出を設定します。サーバー検出間隔を40秒に設定し、到達可能性ステータスが変更された場合にログメッセージを送信します。

[AC-portal-server-newpt] server-detect timeout 40 log

[AC-portal-server-newpt] quit

注:

timeoutの値は、ポータルサーバーのハートビート間隔以上である必要があります。

#ポータルWebサーバーを設定します。

[AC] portal web-server newpt

[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

[AC-portal-websvr-newpt] quit

#VLANインターフェイス100上で直接ポータル認証をイネーブルにします。

[AC] interface vlan-interface 100

[AC–Vlan-interface100] portal enable method direct

#ポータル認証サーバーnewptのポータル失敗許可をイネーブルにします。

[AC–Vlan-interface100] portal fail-permit server newpt

VLAN-interface 100上にポータルWebサーバーnewptを設定します。

[AC–Vlan-interface100] portal apply web-server newpt

#VLANインターフェイス100からポータル認証サーバーに送信されるポータルパケットのBAS-IPを2.2.2.1に設定します。

[AC–Vlan-interface100] portal bas-ip 2.2.2.1

[AC–Vlan-interface100] quit

設定の確認

#ポータル認証サーバーに関する情報を表示します。

[AC] display portal server newpt

Portal server: newpt

IP: 192.168.0.111

VPN instance: Not configured

Port: 50100

Server Detection: Timeout 40s Action: log User

synchronization : Not configured

Status: Up

ポータル認証サーバーのUpステータスは、ポータル認証サーバーが到達可能であることを示します。アクセスデバイスによってポータル認証サーバーが到達不能であることが検出されると、コマンド出力のStatusフィールドにはDownと表示されます。アクセスデバイスによってサーバー到達不能ログPortal server newpt turns down from upldapが生成され、アクセスインターフェイスでポータル認証が無効になるため、ホストは認証なしで外部ネットワークにアクセスできます。

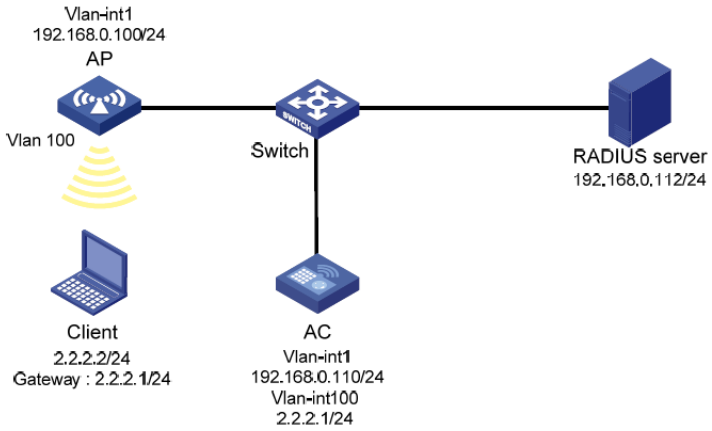
例:ローカルポータルのWebサービスを使用した直接ポータル認証の構成

ネットワーク構成

図20に示すように、クライアントはAPを介してACに接続されています。クライアントには、パブリックIPアドレスが手動またはDHCPを介して割り当てられています。ACはポータル認証サーバーとポータルWebサーバーの両方として機能します。RADIUSサーバーは認証/アカウンティングサーバーとして機能します。

ACで直接ポータル認証を構成します。ユーザーがポータル認証を渡す前は、ユーザーはポータルWebサーバーにのみアクセスできます。ポータル認証を渡した後は、ユーザーは他のネットワークリソースにアクセスできます。

図20 ネットワーク図



前提条件

認証ページをカスタマイズしてファイルに圧縮し、ACのストレージメディアのルートディレクトリにファイルをアップロードします。

RADIUSサーバーの設定

#認証およびアカウンティング機能を提供するようにRADIUSサーバーを正しく設定します(詳細は省略します)。

ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できることを確認します(詳細は省略します)。
2. RADIUSスキームを設定します。

   #rs1という名前のRADIUSスキームを作成し、そのビューに入ります。

   <AC> system-view

   [AC] radius scheme rs1

   #プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

   [AC-radius-rs1] primary authentication 192.168.0.112

   [AC-radius-rs1] primary accounting 192.168.0.112

[AC-radius-rs1] key authentication simple radius

[AC-radius-rs1] key accounting simple radius

#RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

[AC-radius-rs1] user-name-format without-domain

[AC-radius-rs1] quit

#RADIUSセッション制御をイネーブルにします。

[AC] radius session-control enable

3. 認証ドメインを構成します。

#dm1という名前のISPドメインを作成し、そのビューに入ります。

[AC] domain dm1

#ISPドメインのAAA方式を設定します。

[AC-isp-dm1] authentication portal radius-scheme rs1

[AC-isp-dm1] authorization portal radius-scheme rs1

[AC-isp-dm1] accounting portal radius-scheme rs1

[AC-isp-dm1] quit

#ドメインdm1をデフォルトのISPドメインとして構成します。ユーザーがログイン時にISPドメイン名なしでユーザー名を入力した場合、デフォルトメインの認証および会計方法がユーザーに使用されます。

[AC] domain default enable dm1

4. ポータル認証の構成:

#ポータルWebサーバーを構成します。

[AC] portal web-server newpt

[AC-portal-websvr-newpt] url http://2.2.2.1:2331/portal

[AC-portal-websvr-newpt] quit

#VLANインターフェイス100上で直接ポータル認証をイネーブルにします。

[AC] interface vlan-interface 100

[AC–Vlan-interface100] portal enable method direct

VLAN-interface 100上にポータルWebサーバーnewptを設定します。

[AC–Vlan-interface100] portal apply web-server newpt

[AC–Vlan-interface100] quit

#HTTPベースのローカルポータルWebサービスを作成し、そのビューに入ります。

[AC] portal local-web-server http

#ローカルポータルWebサービスのデフォルトの認証ページファイルとしてfile defaultfile.zipを指定します(ファイルがACのルートディレクトリに存在することを確認してください)。

[AC–portal-local-websvr-http] default-logon-page defaultfile.zip

#ローカルポータルWebサービスのHTTPリスニングポート番号を2331に設定します。

[AC-portal-local-websvr-http] tcp-port 2331

[AC-portal-local-websvr-http] quit

宛先ベースのポータルフリー規則1および2を設定して、ポータルユーザーが認証無しにDNSにアクセスできるようにします。

[AC] portal free-rule 1 destination ip any udp 53

[AC] portal free-rule 2 destination ip any tcp 53

5. (任意)client forwarding-location ap(ユーザーデータをCAPWAPトンネルを通さずに、直接VLAN内を通す設定)の場合、以下のコマンドが必要。

[AC] portal host-check enable

設定の確認

#ポータル構成が有効になっていることを確認します。

[AC] display portal interface vlan-interface 100 Portal

information of Vlan-interface 100

VSRP instance:

-- VSRP state:

N/A

AuthorizationStrict checking

ACLDisabled

User profileDisabled Dual stack:

Disabled

Dual traffic-separate: Disabled

IPv4:

Portal status: Enabled

Portal authentication method: Direct Portal

Web server: newpt(active)

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

Pre-auth domain: Not

configured User-dhcp-only:

Disabled

Pre-auth IP pool: Not configured

Max portal users: Not

configured Bas-ip: Not

configured

User Detection: Not

configured Action for server

detection:

Server type Server nameAction

Layer3 source network:

IP addressMask

Destination authenticate subnet:

IP addressMask

IPv6:

Portal status: Disabled

Portal authentication method: Disabled

Portal Web server: Not configured

Secondary portal Web server: Not configured

Portal mac-trigger-server: Not configured

Authentication domain: Not configured

Pre-auth domain: Not

configured User-dhcp-only:

Disabled

Pre-auth IP pool: Not configured

Max portal users: Not

configured Bas-ipv6: Not

configured

User detection: Not

configured Action for server

detection:

Server type Server nameAction

Layer3 source network:

IP addressPrefix length

Destination authenticate subnet:

IP addressPrefix length

ユーザーは、Webページを介してポータル認証を実行できます。認証を渡す前に、ユーザーは認証ページhttp://2.2.2.1:2331/portalにのみアクセスでき、すべてのWeb要求は認証ページにリダイレクトされます。認証を渡した後、ユーザーは他のネットワークリソースにアクセスできます。

#ユーザーが認証にパスした後、ポータルユーザーに関する情報を表示します。

[AC] display portal user interface vlan-interface 100 Total

portal users: 1

Username: abc

Portal server:

newpt State:

Online

VPN instance: --

MAC	IP	VLAN	Interface
0015-e9a6-7cfe	2.2.2.2	--	Vlan-interface100

Authorization information:

IP pool: N/A

User profile: N/A

Session group profile:

N/A ACL: N/A

例:リモートMACベースのクイックポータル認証の設定

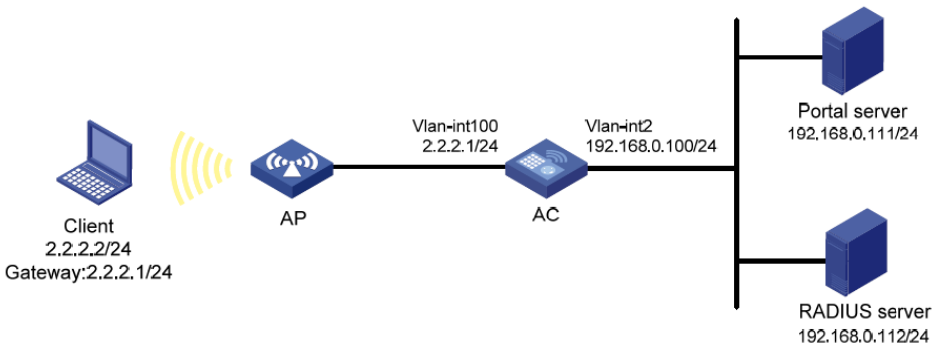
ネットワーク構成

図21に示すように、クライアントはAPを介してWLANにアクセスします。クライアントには、手動またはDHCPを介してパブリックIPアドレスが割り当てられます。iMCサーバーは、ポータル認証サーバー、ポータルWebサーバーおよびMACバインディングサーバーとして機能します。RADIUSサーバーは、認証/会計サーバーとして機能します。この例では、iMCサーバーはiMC PLAT7.1(E0303)およびIMC UAM7.1(E0303)を実行します。

次の要件を満たすように、リモートMACベースのクイックポータル認証を設定します。

- ユーザーのネットワークトラフィックが1024000バイトに達する前に、ユーザーはポータル認証なしでネットワークにアクセスできます。
- ユーザーが初めてポータル認証をパスした後、クライアントはユーザー名またはパスワードを入力せずにポータル認証をパスできます。

図21 ネットワーク図



RADIUSサーバーの設定

#認証およびアカウンティング機能を提供するようにRADIUSサーバーを正しく設定します(詳細は省略します)。

ポータルサーバーの構成

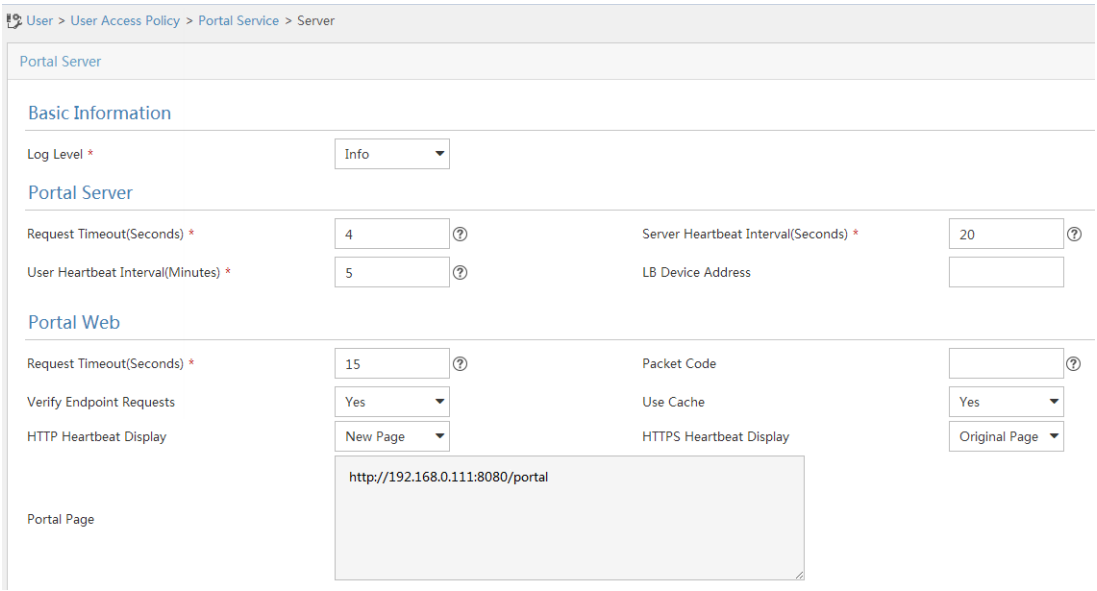
1. ポータルサーバーを構成します。
   a. iMCにログインして、Userタブをクリックします。
   b. 図22に示すように、ナビゲーションツリーからUser Access Policy > Portal Service > Server

を選択して、ポータルサーバーの構成ページを開きます。

c. 必要に応じてポータルサーバーパラメータを構成します。この例ではデフォルト値を使用しています。

d. OKをクリックします。

図22 Portal認証サーバーの構成



2. 次のようにIPアドレスグループを設定します。

a. ナビゲーションツリーからUser Access Policy > Portal Service > IP Groupを選択して、ポータルIPアドレスグループの設定ページを開きます。

b. 図23に示すように、Addをクリックしてページを開きます。

c. IPグループ名を入力します。

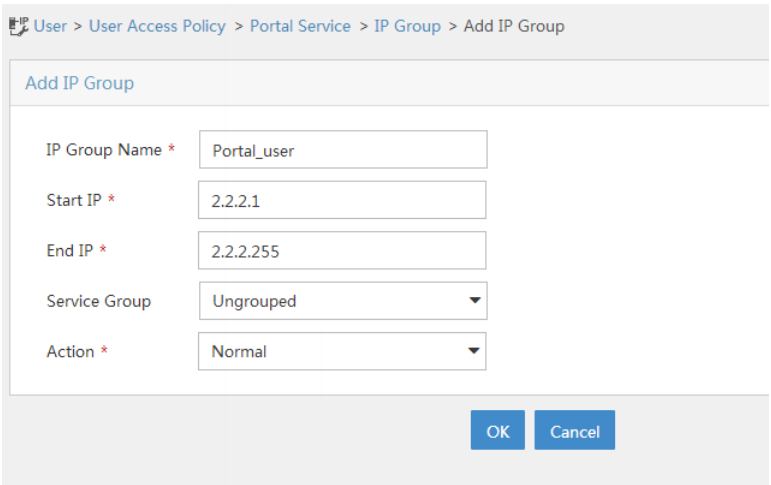
d. IPグループの開始IPアドレスと終了IPアドレスを入力します。クライアントIPアドレス(2.2.2.2)がIPグループ内にあることを確認します。

e. サービスグループを選択します。
この例では、既定のグループUngroupedを使用します。

f. ActionリストからNormalを選択します。

g. OKをクリックします。

図23 IPアドレスグループの追加



3. ポータルデバイスを追加します。

   a. ナビゲーションツリーからUser Access Policy > Portal Service > Deviceを選択して、ポータルデバイスの設定ページを開きます。

   b. 図24に示すように、Addをクリックしてページを開きます。

   c. デバイス名を入力します。

   d. クライアントに接続されているACのインターフェイスのIPアドレスを入力します。

   e. ポータルサーバーのハートビートおよびユーザーのハートビート機能をサポートするかどうかを設定します。

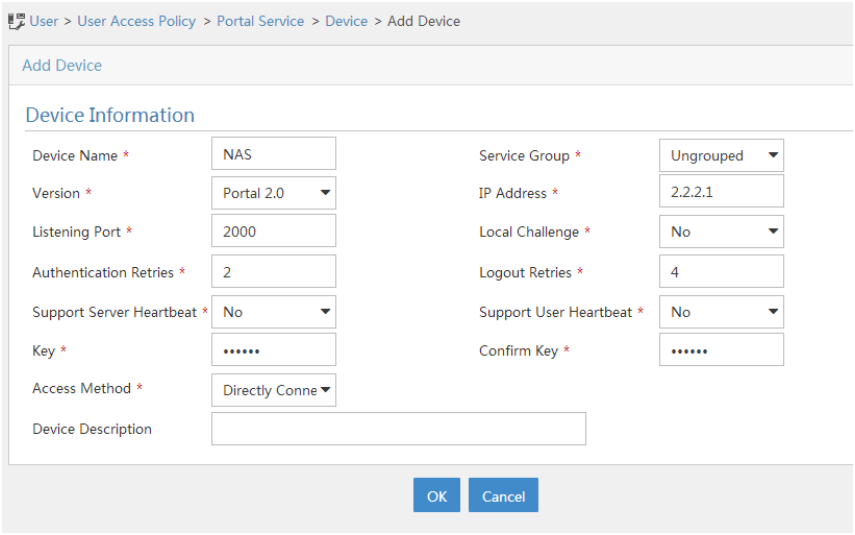
      この例では、Support Server HeartbeatとSupport User Heartbeatの両方に対してNoを選択します。

   f. キーを入力します。キーは、ACに設定されているキーと同じである必要があります。

   g. Access MethodリストからDirectly Connectedを選択します。

   h. OKをクリックします。

図24 ポータルデバイスの追加



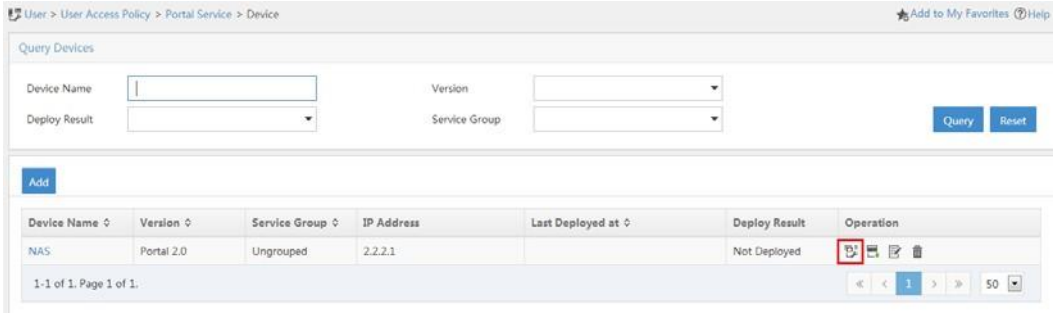
4. ポータルデバイスをIPアドレスグループに関連付けます。

   a. 図25に示すように、デバイスのPort Group Information Managementアイコンをクリックします。

      NAS: ポートグループの構成ページを開きます。

図25 デバイスリスト



b. 図26に示すように、Addをクリックしてページを開きます。

c. ポートグループ名を入力します。

d. 設定済みのIPアドレスグループを選択します。

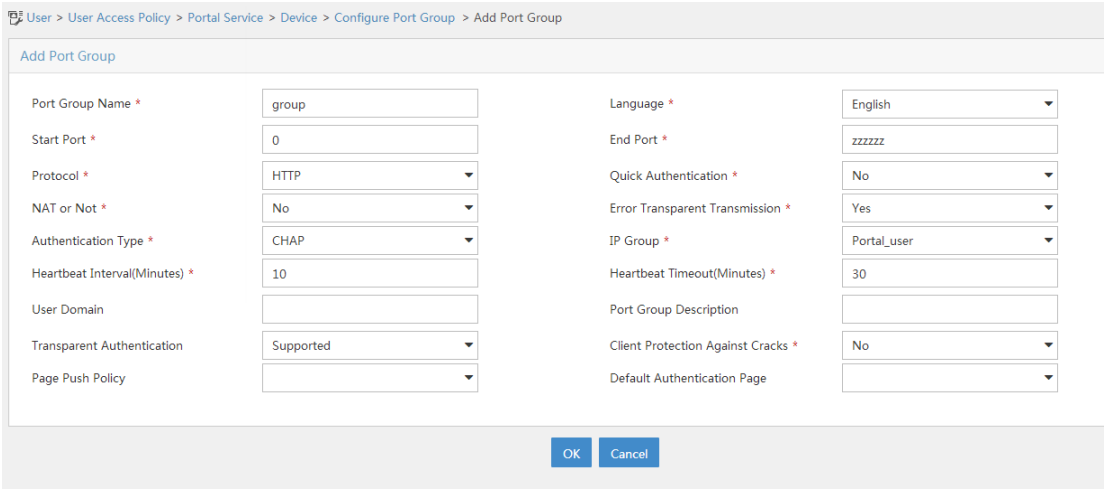
ユーザーがネットワークにアクセスするために使用するIPアドレスは、このIPアドレスグループ内にある必要があります。

e. Supported for Transparent Authenticationを選択します。

f. その他のパラメータにはデフォルト設定を使用します。

g. OKをクリックします。

図26 ポートグループの追加



MACバインディングサーバーの設定

1. アクセスポリシーを追加します:

a. ナビゲーションツリーからUser Access Policy>Access Policyを選択して、アクセスポリシーページを開きます。

b. 図27に示すように、Addをクリックしてページを開きます。

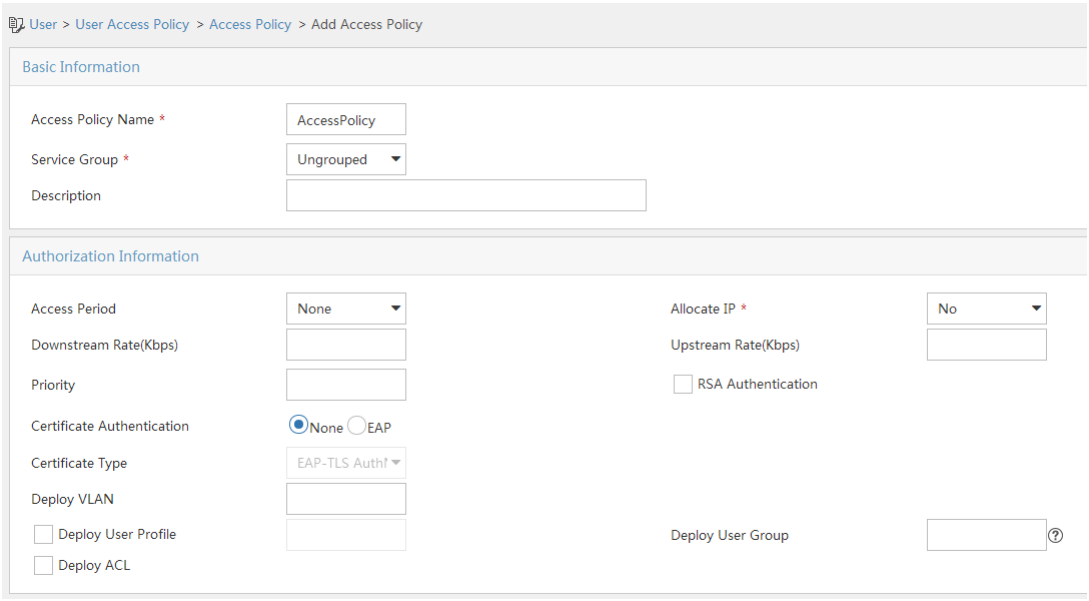
c. アクセスポリシー名を入力します。

d. サービスグループを選択します。

e. その他のパラメータにはデフォルト設定を使用します。

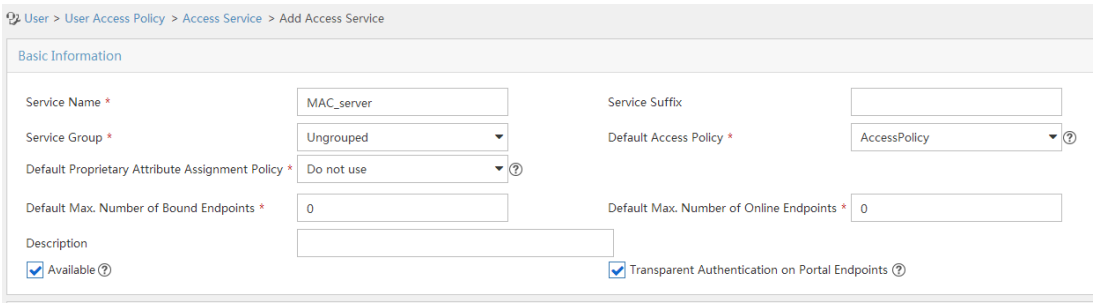
f. OKをクリックします。

図27アクセスポリシーの追加



2. アクセスサービスを追加します。
   a. ナビゲーションツリーからUser Access Policy > Access Serviceを選択して、アクセスサービスページを開きます。
   b. 図28に示すように、Addをクリックしてページを開きます。
   c. サービス名を入力します。
   d. Transparent Authentication on Portal Endpointsオプションを選択します。
   e. その他のパラメータにはデフォルト設定を使用します。
   f. OKをクリックします。

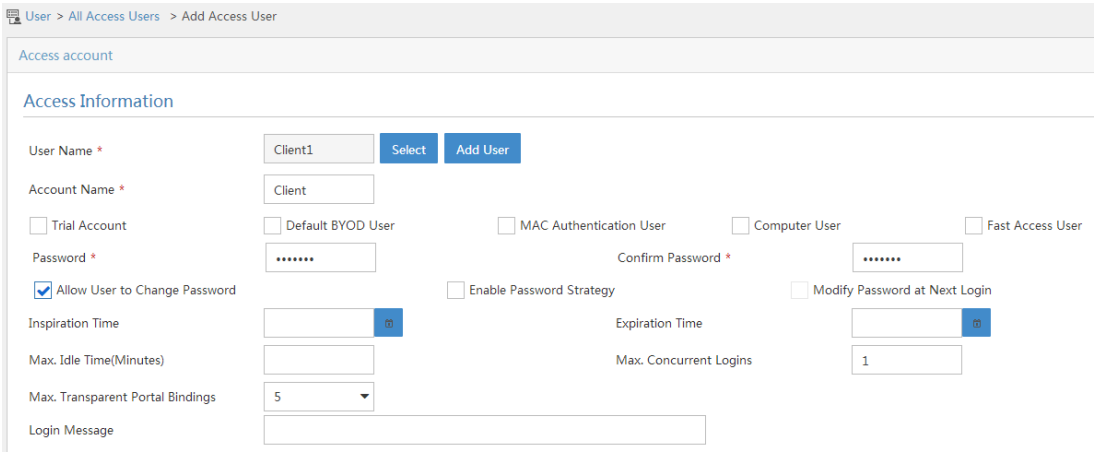
図28 アクセスサービスの追加



3. アクセスユーザーを追加します。
   a. ナビゲーションツリーからAccess User > All Access Usersを選択して、アクセスユーザーページを開きます。
   b. 図29に示すように、Addをクリックしてページを開きます。
   c. アクセスユーザーを選択します。
   d. パスワードを設定します。
   e. Max.Transparent Portal Bindingsリストから値を選択します。

f. OKをクリックします。

図29 アクセスユーザーの追加



4. システムパラメータを設定します。

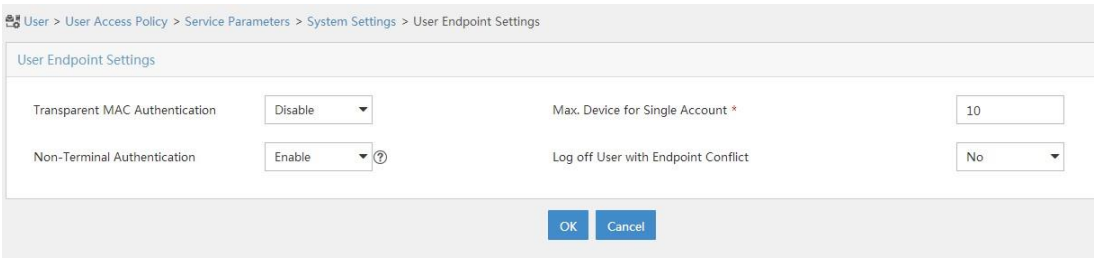
a. ナビゲーションツリーからUser Access Policy > Service Parameters > System Settingsを選択して、システム設定ページを開きます。

b. 非スマートデバイスで透過的ポータル認証を使用可能にするかどうかを選択します。

この例では、Non-Terminal Authenticationに対してEnableを選択します。

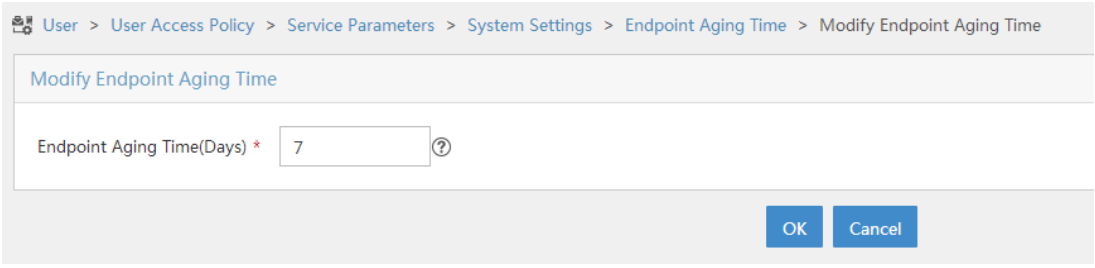
c. OKをクリックします。

図30 ユーザーエンドポイント設定の構成



d. 必要に応じて、エンドポイントのエージングタイムを設定します。この例ではデフォルト値を使用します。

図31 エンドポイントのエージングタイムの設定



ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できる

ことを確認します(詳細は省略します)。

2. RADIUSスキームを設定します。

   #rs1という名前のRADIUSスキームを作成し、そのビューに入ります。

   <AC> system-view

   [AC] radius scheme rs1

   #プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

   [AC-radius-rs1] primary authentication 192.168.0.112

   [AC-radius-rs1] primary accounting 192.168.0.112

   [AC-radius-rs1] key authentication simple radius

   [AC-radius-rs1] key accounting simple radius

   #RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

   [AC-radius-rs1] user-name-format without-domain

   [AC-radius-rs1] quit

   #RADIUSセッション制御をイネーブルにします。

   [AC] radius session-control enable

3. 認証ドメインを構成します。

   #dm1という名前のISPドメインを作成し、そのビューに入ります。

   [AC] domain dm1

   #ISPドメインのAAA方式を設定します。

   [AC-isp-dm1] authentication portal radius-scheme rs1

   [AC-isp-dm1] authorization portal radius-scheme rs1

   [AC-isp-dm1] accounting portal radius-scheme rs1

   [AC-isp-dm1] quit

   #ドメインdm1をデフォルトのISPドメインとして構成します。ユーザーがログイン時にISPドメイン名なしでユーザー名を入力した場合、デフォルトドメインの認証および会計方法がユーザーに使用されます。

   [AC] domain default enable dm1

4. ポータル認証を構成します。

   # ポータル認証サーバーを構成します。

   [AC] portal server newpt

   [AC-portal-server-newpt] ip 192.168.0.111 key simple portal

   [AC-portal-server-newpt] port 50100

   [AC-portal-server-newpt] quit

   # ポータルWebサーバーを設定します。

   [AC] portal web-server newpt

   [AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal

[AC-portal-websvr-newpt] quit

#ワイヤレスクライアントで妥当性チェックを有効にします。

[AC] portal host-check enable

#st1という名前のサービステンプレートを作成し、SSIDをst1に設定して、サービステンプレートにVLAN100を作成します。

[AC] wlan service-template st1

[AC-wlan-st-st1] ssid st1

[AC-wlan-st-st1] vlan 100

#サービステンプレートst1で直接認証をイネーブルにします。

[AC–wlan-st-st1] portal enable method direct

#サービステンプレートst1のポータルWebサーバーnewptを指定します。

[AC–wlan-st-st1] portal apply web-server newpt

#サービステンプレートst1からポータル認証サーバーに送信されるポータルパケットのBAS-IPを2.2.2.1に設定します。

[AC-wlan-st-st1] portal bas-ip 2.2.2.1

[AC-wlan-st-st1] quit

5. MACベースのクイックポータル認証を構成します。

mtsという名前のMACバインディングサーバーを作成します。

[AC] portal mac-trigger-server mts

ポータルユーザーの空きトラフィックのしきい値を1024000バイトに設定します。

[AC-portal-mac-trigger-server-mts] free-traffic threshold 1024000

MACバインディングサーバーのIPアドレスを192.168.0.111に指定します。

[AC-portal-mac-trigger-server-mts] ip 192.168.0.111

[AC-portal-mac-trigger-server-mts] quit

サービステンプレートst1のMACバインディングサーバーmtsを指定します。

[AC] wlan service-template st1

[AC-wlan-st-st1] portal apply mac-trigger-server mts

サービステンプレートst1を有効にします。

[AC-wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

設定の確認

#MACバインディングサーバーに関する情報を表示します。

[AC] display portal mac-trigger-server name mts

Portal mac-trigger server: mts Version: 1.0

Server type: iMC

IP: 192.168.0.111

Port: 50100

VPN instance: Not configured

Aging time: 300 seconds Free-traffic threshold:
1024000 bytes NAS-Port-Type: Not configured
Binding retry times: 3 Binding retry interval: 1
seconds Authentication timeout: 3 minutes

ユーザーは、H3C iNodeクライアントまたはWebブラウザを使用してポータル認証を実行できます。認証を渡す前にアクセスできるのは、認証ページhttp://192.168.0.111:8080/portalのみです。ユーザーからのすべてのWeb要求は、認証ページにリダイレクトされます。認証を渡した後、ユーザーは他のネットワークリソースにアクセスできます。

最初のポータル認証では、ユーザーはユーザー名とパスワードを入力する必要があります。ユーザーがオフラインになり、再度ネットワークにアクセスする場合、ユーザーは認証ユーザー名とパスワードを入力する必要はありません。

#ポータルユーザー情報を表示します。

[AC] display portal user all Total
portal users: 1
Username: Client1
AP name: ap1
Radio ID: 1
SSID:st1
Portal server: newpt
State: Online
VPN instance: N/A
MACIPVLANInterface
0015-e9a6-7cfe2.2.2.2100WLAN-BSS1/0/1
Authorization information:
DHCP IP pool: N/A
User profile: N/A
Session group profile: N/A ACL
number/name: N/A
CAR: N/A

例:ローカルMACベースのクイックポータル認証の設定

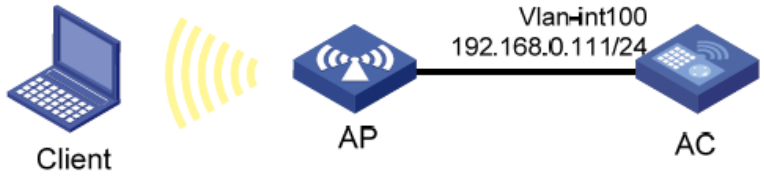
ネットワーク構成

図32に示すように、クライアントはAPを介してWLANにアクセスします。クライアントには、手動またはDHCPを介してパブリックIPアドレスが割り当てられます。ACは、ポータル認証サーバー、ポータルWebサーバー、およびMACバインディングサーバーとして機能します。

次の要件を満たすように、ローカルMACベースのクイックポータル認証を設定します。

- ユーザーのネットワークトラフィックが1024000バイトに達する前に、ユーザーはポータル認証なしでネットワークにアクセスできます。
- クライアントは、ユーザーがポータル認証に初めてパスしてから24分以内に、ユーザー名またはパスワードを入力せずにポータル認証をパスできます。

図32 ネットワーク図



手順

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できることを確認します(詳細は省略します)。
2. 認証ドメインを設定します。#dm1という名前のISPドメインを作成します。

   <AC> system-view

   [AC] domain dm1

   # ISPドメインdm1内のポータルユーザーのローカル認証、許可、およびアカウンティングを構成する

   [AC-isp-dm1] authentication portal local

   [AC-isp-dm1] authorization portal local

   [AC-isp-dm1] accounting portal local

   [AC-isp-dm1] quit

   # ISPドメインdm1をデフォルトのISPドメインとして設定します。

   [AC] domain default enable dm1
3. ポータル認証を構成します。

   # ポータルWebサーバーnewptを作成し、ポータルWebサーバーのURLを次のように構成します。
   http://192.168.0.111/portal

   [AC] portal web-server newpt

   [AC-portal-websvr-newpt] url http://192.168.0.111/portal

   [AC-portal-websvr-newpt] quithttp://192.168.0.111/portal

   # ワイヤレスポータルクライアントで妥当性チェックを有効にします。

   [AC] portal host-check enable

   # st1という名前のサービステンプレートを作成します。

   [AC] wlan service-template st1

   [AC-wlan-st-st1] ssid st1

   # サービステンプレートst1で直接IPv4ポータル認証をイネーブルにします。

   [AC-wlan-st-st1] portal enable method direct

   # サービステンプレートst1のポータルWebサーバーnewptをポータル認証用に指定します。

   [AC-wlan-st-st1] portal apply web-server newpt

   [AC-wlan-st-st1] quit
4. ローカルMACベースのクイックポータル認証を設定します。

   # mtsという名前のMACバインディングサーバーを作成します。

[AC] portal mac-trigger-server mts

ローカルMACベースのクイックポータル認証をイネーブルにします。

[AC-portal-mac-trigger-server-mts] local-binding enable

ポータルユーザーの空きトラフィックのしきい値を1024000バイトに設定します。

[AC-portal-mac-trigger-server-mts] free-traffic threshold 1024000

ローカルMACアカウントバインディングエントリのエージングタイムを24分に設定します。

[AC-portal-mac-trigger-server-mts] local-binding aging-time 24

[AC-portal-mac-trigger-server-mts] quit

サービステンプレートst1にMACバインディングサーバーmtsを指定します。

[AC] wlan service-template st1

[AC-wlan-st-st1] portal apply mac-trigger-server mts

サービステンプレートst1を有効にします。

[AC-wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

HTTPベースのローカルポータルWebサービスを作成し、そのビューに入ります。

[AC] portal local-web-server http

ポータル認証用のデフォルトの認証ページファイルとしてfile defaultfile.zipを指定します(ファイルがACのルートディレクトリに存在することを確認してください)。

[AC–portal-local-websvr-http] default-logon-page defaultfile.zip

[AC–portal-local-websvr-http] quit

5. ローカルユーザーを構成します。

client1という名前のネットワークアクセスユーザーを作成し、そのユーザーのパスワードをpasswordに設定します。プレーンテキスト形式で保存されます。

[AC] local-user client1 class network

[AC-luser-network-client1] password simple password

[AC-luser-network-client1] quit

宛先ベースのポータルフリー規則1および2を設定して、ポータルユーザーが認証無しにDNSにアクセスできるようにします。

[AC] portal free-rule 1 destination ip any udp 53

[AC] portal free-rule 2 destination ip any tcp 53

6. (任意)client forwarding-location ap(ユーザーデータをCAPWAPトンネルを通さずに、直接VLAN内を通す設定)の場合、以下のコマンドが必要。

[AC] portal host-check enable

設定の確認

#MACバインディングサーバーmtsに関する情報を表示します。

[AC]display portal mac-trigger-server name mts Portal mac-trigger server:mts

Version: 1.0

Server type: iMC

IP: 192.168.0.111

Port: 50100

VPN instance: Not configured

Aging time: 300 seconds Free-traffic

threshold: 1024000 bytes NAS-Port-Type:

Not configured

Binding retry times: 3 Binding retry

interval: 1 seconds Authentication

timeout: 3 minutes Local-binding:

Enabled

Local-binding aging-time: 24 minutes

aaa-fail nobinding: Disabled

Excluded attribute list: Not configured

Cloud-binding: Disabled

Cloud-server URL: Not configured

ユーザーは、H3C iNodeクライアントまたはWebブラウザを使用してポータル認証を実行できます。認証を渡す前にアクセスできるのは、認証ページhttp://192.168.0.111/portalのみです。ユーザーからのすべてのWeb要求は、認証ページにリダイレクトされます。認証を渡した後、ユーザーは他のネットワークリソースにアクセスできます。http://192.168.0.111/portal

最初のポータル認証では、ユーザーはユーザー名とパスワードを入力する必要があります。ユーザーがオフラインになり、再度ネットワークにアクセスする場合、ユーザーは認証ユーザー名とパスワードを入力する必要はありません。

ローカルMACアカウントバインディングエントリに関する情報を表示します。

[AC]display portal local-binding mac-address all Total mac-address number:1

Mac-addressUser-name

0800-2700-b43aclient1

#vlan-interface100上のポータルユーザーに関する情報を表示します。

[AC]display portal user interface vlan-interface100

Total number of portal users:1

Username: client1

Portal server:

N/A State:

Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0800-2700-b43a	192.168.0.56	100	WLAN-BSS1/0/1

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile:

N/A ACL number/name:

N/A

CAR: N/A

例:クラウドMACトリガー認証の設定

ネットワーク構成

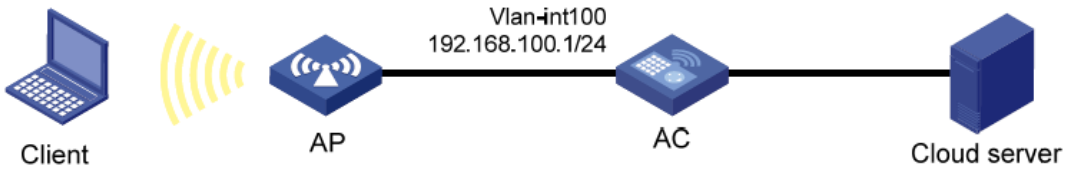
図33に示すように:

- ACはDHCPサーバーとして機能し、クライアントにプライベートIPアドレスを割り当てます。クライアントはプライベートIPアドレスを使用してポータル認証を実行します。
- クラウドサーバーは、ポータル認証サーバー、ポータルWebサーバー、およびMACバインディングサーバーとして機能します。

次の要件を満たすように、クラウドMACトリガー認証を設定します。

- ユーザーは、ポータル認証を渡す前にポータルWebサーバーにのみアクセスできます。
- ユーザーは、ポータル認証を受けた後にネットワークリソースにアクセスできます。ユーザーは、ユーザーが再びオンラインになろうとしたときに、ユーザー名またはパスワードを入力せずにポータル認証を受け渡すことができます。

図33 ネットワーク図



クラウドサーバーの設定

#Oasisプラットフォームでは、ACの認証テンプレートにAuth freeを有効にして再接続します(詳細は省略します)。

ACの設定

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびサーバーが相互に到達できることを確認します(詳細は省略します)。
2. 基本的なネットワーク機能を設定します。

   #VLAN100を作成します。クライアントはVLAN100を介してワイヤレスネットワークにアクセスします。

   <AC> system-view

   [AC] vlan 100

   [AC-vlan100] quit

   # VLANインターフェイスにIPアドレスを割り当てます(詳細は省略します)。

   # DNSプロキシをイネーブルにします。

   [AC] dns proxy enable

DHCPを有効にします。

[AC] dhcp enable

#clientという名前のDHCPアドレスプールを作成します。

[AC] dhcp server ip-pool client

サブネット192.168.100.0/24.からクライアントにIPアドレスを割り当てるようにDHCPアドレスプールクライアントを設定します。

[AC-dhcp-pool-client] network 192.168.100.0 mask 255.255.255.0

ダイナミック割り当てからIPアドレス192.168.100.1を除外します。

[AC-dhcp-pool-client] forbidden-ip 192.168.100.1

ゲートウェイアドレスとして192.168.100.1を指定します。

[AC-dhcp-pool-client] gateway-list 192.168.100.1

192.168.100.1をDNSサーバーアドレスとします。

[AC-dhcp-pool-client] dns-list 192.168.100.1

[AC-dhcp-pool-client] quit

VLANインターフェイス100にDHCPアドレスプールクライアントを適用します。

[AC] interface vlan-interface 100

[AC-Vlan-interface100] dhcp server apply ip-pool client

[AC-Vlan-interface100] quit

3. 次の手順に従って、ISPドメインを設定します。

cloudという名前のISPドメインを作成します。

[AC] domain cloud

ポータルユーザーに対して認証、認可、またはアカウンティングを実行しないようにACを設定します。

[AC-isp-cloud] authentication portal none

[AC-isp-cloud] authorization portal none

[AC-isp-cloud] accounting portal none

[AC-isp-cloud] quit

4. クラウドMACトリガー認証を設定します。

wbsという名前のポータルWebサーバーを作成します。

[AC]portal web-server wbs

ポータルWebサーバーwbsのURLとしてhttp://oasisauth.h3c.comを指定します。
http://oasisauth.h3c.com/

[AC-portal-websvr-wbs] url http://oasisauth.h3c.comhttp://oasisauth.h3c.com/

ポータルWebサーバーのタイプをoauthとして指定します。

[AC-portal-websvr-wbs] server-type oauth

ポータルのキャプティブバイパス機能をイネーブルにします。

[AC-portal-websvr-wbs] captive-bypass enable

一時パスルールを設定して、URLhttp://oasisauth.h3c.comにアクセスするユーザーパケットを一時的に許可します。http://oasisauth.h3c.com/

[AC-portal-websvr-wbs] if-match original-url http://oasisauth.h3c.com temp-pass

[AC-portal-websvr-wbs] quithttp://oasisauth.h3c.com/

クラウドMACトリガー認証をイネーブルにします。

[AC] portal mac-trigger-server abc

[AC-portal-extend-auth-server-abc] cloud-binding enable

クラウドポータル認証サーバーのURLとしてhttp://oasisauth.h3c.comを指定します。

[AC-portal-extend-auth-server-abc]cloud-server url http://oasisauth.h3c.com

[AC-portal-extend-auth-server-abc]quithttp://oasisauth.h3c.com/http://oasisauth.h3c.com/

st1という名前のサービステンプレートを作成します。

[AC] wlan service-template st1

サービステンプレートst1を介してオンラインになるクライアントをVLAN100に割り当てます。

[AC-wlan-st-st1] vlan 100

サービステンプレートst1のSSIDをcloudに設定します。

[AC-wlan-st-st1] ssid cloud

#サービステンプレートst1で直接ポータル認証を有効にします。

[AC-wlan-st-st1] portal enable method direct

#ISPドメインクラウドをポータル認証ドメインとして指定します。

[AC-wlan-st-st1] portal extend-auth domain extend-auth

#サービステンプレートst1のポータルWebサーバーwbsを指定します。

[AC-wlan-st-st1] portal apply web-server wbs

#サービステンプレートst1にMACバインディングサーバーabcを指定します。

[AC-wlan-st-st1] portal apply mac-trigger-server abc

#ポータルの一時パスを有効にし、一時パスの期間を60秒に設定します。

[AC-wlan-st-st1] portal temp-pass period 60 enable

#サービステンプレートst1を有効にします。

[AC-wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

#モデルWA2620i-AGNでAP lvzhou-apを作成し、そのシリアルIDを219801A0CNC123001072に設定します。

[AC] wlan ap lvzhou-ap model WA2620i-AGN

[AC-wlan-ap-lvzhou-ap] serial-id 219801A0CNC123001072

#radio1のビューに入ります。

[AC-wlan-ap-ap1] radio 1

#サービステンプレートst1をradio1にバインドします。

[AC-wlan-ap-ap1-radio-1] service-template st1

#radio1を有効にします。

[AC-wlan-ap-ap1-radio-1] radio enable

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

#宛先ベースのポータルフリー規則1および2を構成して、ポータルユーザーが認証なしでDNSサービスにアクセスできるようにします。

[AC] portal free-rule 1 destination ip any udp 53

[AC] portal free-rule 2 destination ip any tcp 53

#(任意)client forwarding-location ap(ユーザーデータをCAPWAPトンネルを通さずに、直接VLAN内を通す設定)の場合、以下のコマンドが必要。

[AC] portal host-check enable

設定の確認

#クラウドポータル認証サーバーのパケット統計情報を表示します。

[AC] display portal packet statistics extend-auth-server cloud Extend-auth server : cloud

Pkt-TypeSuccessErrorTimeoutConn-failure REQ_ACCESSTOKEN1000
REQ_USERINFO1000

RESP_ACCESSTOKEN	1	0	0	0
RESP_USERINFO	1	0	0	0
POST_ONLINEDATA	10	0	0	0
RESP_ONLINEDATA	10	0	0	0
POST_OFFLINEUSER	1	0	0	0
REPORT_ONLINEUSER	2	0	0	0
REQ_CLOUDBIND	2	0	0	0
ESP_CLOUDBIND	2	0	0	0
REQ_BINDUSERINFO	1	0	0	0
RESP_BINDUSERINFO	1	0	0	0
AUTHENTICATION	2	0	0	0

ポータル認証を渡す前に、ユーザーはポータル認証ページhttp://oasisauth.h3c.comにのみアクセスできます。ユーザーからのすべてのWeb要求は、ポータル認証ページにリダイレクトされます。ポータル認証を渡すと、ユーザーは他のネットワークリソースにアクセスできます。http://oasisauth.h3c.com/

ユーザーは、最初の認証のためにユーザー名とパスワードを入力する必要があります。ユーザーがオフラインになり、オンラインになろうとすると、ユーザー名とパスワードを入力しなくてもネットワークリソースに直接アクセスできます。

#すべてのポータルユーザーに関する情報を表示します。

[AC] display portal user all

Total portal users: 1

Username: client1

AP name:

lvzhou-ap Radio

ID: 2

SSID: WXauth

Portal server:

N/A State:

Online

VPN instance: N/A

MAC	IP	VLAN	Interface
582a-f776-8050	192.168.100.3	100	WLAN-BSS2/0/5

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile:

N/A ACL number/name:

N/A Inbound CAR: N/A

Outbound CAR: N/A

例:QQ認証のポータルサポートの設定

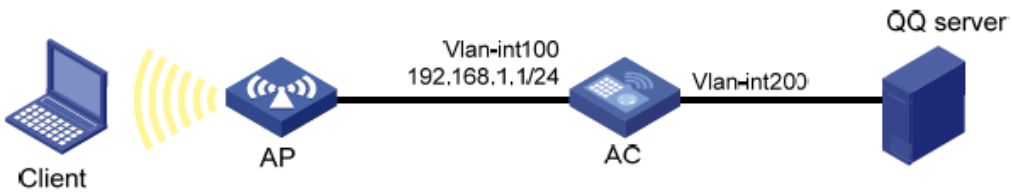
ネットワーク構成

図34に示すように、ACはDHCPサーバーとして機能し、クライアントにプライベートIPアドレスを割り当てます。クライアントはプライベートIPアドレスを使用してQQ認証を実行します。

次の要件を満たすように、QQ認証のポータルサポートを設定します。

- クライアントはQQ認証を渡す前にQQ認証サーバーにしかアクセスできない。
- クライアントはQQ認証を受けた後、他のネットワークリソースにアクセスすることができます。

図34 ネットワーク図



前提条件

ポータル認証ページを編集し、QQ認証ボタンをログオンページに追加します。認証ページを.zipファイルに圧縮し、認証ページファイルをACのルートディレクトリに保存します。この例では、ファイルabc.zipを使用します。

手順

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびQQサーバーが互いに到達できることを確認します(詳細は省略します)。
2. 基本的なネットワーク機能を設定します。

#VLAN100を作成します。クライアントはVLAN100を介してワイヤレスネットワークにアクセスします。

<AC> system-view

[AC] vlan 100

[AC-vlan100] quit

VLAN200を作成します。ACはこのVLANをNATに使用し、DHCPを介してパブリックIPアドレスを取得します。

[AC] vlan 200

[AC-vlan200] quit

VLANインターフェイスにIPアドレスを割り当てます(詳細は省略します)。

DNSプロキシをイネーブルにします。

[AC] dns proxy enable

IPアドレス192.168.1.1をポータルWebサーバーlvzhou.h3c.comのドメイン名にマッピングします。

[AC] ip host lvzhou.h3c.com 192.168.1.1

DHCPを有効にします。

[AC] dhcp enable

clientという名前のDHCPアドレスプールを作成します。

[AC] dhcp server ip-pool client

サブネット192.168.1.0/24からクライアントにIPアドレスを割り当てるように、DHCPアドレスプールクライアントを設定します。

[AC-dhcp-pool-client] network 192.168.1.0 mask 255.255.255.0

ダイナミック割り当てからIPアドレス192.168.1.1.1を除外します。

[AC-dhcp-pool-client] forbidden-ip 192.168.1.1

ゲートウェイアドレスとして192.168.1.1を指定します。

[AC-dhcp-pool-client] gateway-list 192.168.1.1

192.168.1.1 をDNSサーバーアドレスにします。

[AC-dhcp-pool-client] dns-list 192.168.1.1

[AC-dhcp-pool-client] quit

VLANインターフェイス100にDHCPアドレスプールクライアントを適用します。

[AC] interface vlan-interface 100

[AC-Vlan-interface100] dhcp server apply ip-pool client

[AC-Vlan-interface100] quit

ACL2000を設定し、サブネット192.168.1.0/24から通過するパケットだけを許可するルールを作成します。

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-acl-ipv4-basic-2000] quit

IPアドレスの取得にDHCPを使用するようにVLANインターフェイス200を設定します。

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address dhcp-alloc

インターフェイスVLANインターフェイス200でEasy IPを使用したアウトバウンドNATをイネーブルにします。

[AC-Vlan-interface200] nat outbound 2000

3. 認証ドメインを構成します。

extend-authという名前のISPドメインを作成します。

[AC] domain extend-auth

ポータルユーザーの認証、認可、またはアカウンティングを実行しないようにデバイスを設定します。

[AC-isp-extend-auth] authentication portal none

[AC-isp-extend-auth] authorization portal none

[AC-isp-extend-auth] accounting portal none

[AC-isp-extend-auth] quit

4. QQ認証を設定する:

#ポータルWebサーバーのURLとしてhttp://192.168.1.1/portalを指定します。

[AC] portal web-server wbs

[AC-portal-websvr-wbs] url http://192.168.1.1/portal

[AC-portal-websvr-wbs] quithttp://192.168.1.1/portal

QQ認証サーバーを作成する。

[AC] portal extend-auth-server qq

[AC-portal-extend-auth-server-qq] quit

st1というサービステンプレートを作成します。

[AC] wlan service-template st1

サービステンプレートst1を介してオンラインになるクライアントをVLAN100に割り当てます。

[AC-wlan-st-st1] vlan 100

サービステンプレートst1のSSIDをserviceに設定します。

[AC-wlan-st-st1]ssid service

サービステンプレートst1で直接ポータル認証を有効にします。

[AC-wlan-st-st1] portal enable method direct

QQ認証用の認証ドメインとしてISPドメイン拡張認証を指定します。

[AC-wlan-st-st1] portal extend-auth domain extend-auth

サービステンプレートst1のポータルWebサーバーwbsを指定します。

[AC-wlan-st-st1] portal apply web-server wbs

サービステンプレートst1を有効にします。

[AC-wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

モデルWA4320i-CANを使用してAP ap1を作成し、シリアルIDを210235A29G007C000020に設定します。

[AC] wlan ap ap1 model WA4320i-ACN

[AC-wlan-ap-ap1] serial-id 210235A29G007C000020

radio1のビューに入ります。

[AC-wlan-ap-ap1] radio 1

サービステンプレートst1をradio1にバインドします。

[AC-wlan-ap-ap1-radio-1] service-template st1

radio1を有効にします。

[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

HTTPベースのローカルポータルWebサービスを作成し、そのビューに入ります。

[AC] portal local-web-server http

ローカルポータル認証用のデフォルト認証ページファイルとして、ファイルdefaultfile.zipを指定します。(ファイルがACのルートディレクトリに存在することを確認してください。)

[AC-portal-local-websvr-http] default-logon-page defaultfile.zip

[AC-portal-local-websvr-http] quit

宛先ベースのポータルフリー規則1および2を設定して、ポータルユーザーが認証無しにDNS通過するようにアクセスできるようにします。

[AC] portal free-rule 1 destination ip any udp 53

[AC] portal free-rule 2 destination ip any tcp 53

#(任意)client forwarding-location ap(ユーザーデータをCAPWAPトンネルを通さずに、直接VLAN内を通す設定)の場合、以下のコマンドが必要。

[AC] portal host-check enable

宛先ベースのポータルフリー規則3および4を設定して、ポータルユーザーが認証なしにQQ認証サーバーにアクセスできるようにする。

[AC] portal free-rule 3 destination *.qq.com

[AC] portal free-rule 4 destination *.gtimg.cn

設定の確認

#QQ認証サーバーに関する情報を表示します。

[AC] display portal extend-auth-server all

Portal extend-auth-server: qq

Authentication URL : https://graph.qq.com

APP ID: 101235509

APP key: ******

Redirect URL: http://oauthindev.h3c.com/portal/qqlogin.html
http://oauthindev.h3c.com/portal/qqlogin.html

認証を渡す前に、ユーザーはポータル認証ページhttp://192.168.0.111/portalにのみアクセスできます。ユーザーからのすべてのWeb要求はポータル認証ページにリダイレクトされます。ポータル認証ページでQQ認証ボタンをクリックすると、ユーザーはQQ認証ページにリダイレクトされます。QQ認証を渡すと、ユーザーは他のネットワークリソースにアクセスできます。
http://192.168.0.111/portal

すべてのポータルユーザーに関する情報を表示します。

[AC] display portal user all

Total portal users: 1

Username: 00-00-00-00-00-01

AP name:

ap1 Radio

ID: 1

SSID:servi

ce

Portal server:

N/A State:

Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0015-e9a6-7cfe	192.168.1.2	100	WLAN-BSS1/0/1

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile:

N/A ACL number/name:

N/A

CAR: N/A

例:電子メール認証のポータルサポートの設定

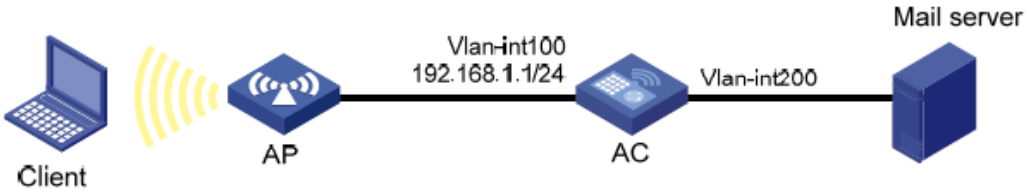
ネットワーク構成

図35に示すように、ACはDHCPサーバーとして機能し、クライアントにプライベートIPアドレスを割り当てます。クライアントはプライベートIPアドレスを使用して電子メール認証を実行します。

次の要件を満たすように、電子メール認証のポータルサポートを構成します。

- クライアントは、認証を渡す前に電子メール認証サーバーにのみアクセスできます。
- クライアントは認証にパスした後、他のネットワークリソースにアクセスできます。

図35 ネットワーク図



前提条件

ポータル認証ページおよび電子メール認証ページを編集し、電子メール認証ボタンをポータルログオンページに追加します。認証ページを.zipファイルに圧縮し、認証ページファイルをACのルートディレクトリに保存します。この例では、ファイルabc.zipを使用しています。

手順

1. インターフェイスにIPアドレスを割り当て、クライアント、AC、およびメールサーバーが相互に到達できることを確認します(詳細は省略します)。
2. 基本的なネットワーク機能を設定します。

   #VLAN100を作成します。クライアントはVLAN100を介してワイヤレスネットワークにアクセスします。

   <AC> system-view

   [AC] vlan 100

   [AC-vlan100] quit

   # VLAN200を作成します。ACはNATにVLAN200を使用し、DHCPを介してパブリックネットワークアドレスを取得します。

   [AC] vlan 200

   [AC-vlan200] quit

   # VLANインターフェイスにIPアドレスを割り当てます(詳細は省略します)。#DNSプロキシをイネーブルにします。

   [AC] dns proxy enable

   # ポータルWebサーバーwww.mail.comのドメイン名とIPアドレス192.168.1.1の間のマッピングを構成します。http://www.mail.com/

   [AC] ip host www.mail.com 192.168.1.1http://www.mail.com/

   # DHCPを有効にします。

   [AC] dhcp enable

   # clientという名前のDHCPアドレスプールを作成します。

   [AC] dhcp server ip-pool client

   # サブネット192.168.1.0/24からクライアントにIPアドレスを割り当てるように、DHCPアドレスプールクライアントを設定します。

   [AC-dhcp-pool-client] network 192.168.1.0 mask 255.255.255.0

   # ダイナミック割り当てからIPアドレス192.168.1.1を除外します。

   [AC-dhcp-pool-client] forbidden-ip 192.168.1.1

   # ゲートウェイアドレスとして192.168.1.1を指定します。

   [AC-dhcp-pool-client] gateway-list 192.168.1.1

192.168.1.1をDNSサーバーアドレスとして設定します。

[AC-dhcp-pool-client] dns-list 192.168.1.1

[AC-dhcp-pool-client] quit

#VLANインターフェイス100にDHCPアドレスプールクライアントを適用します。

[AC] interface vlan-interface 100

[AC-Vlan-interface100] dhcp server apply ip-pool client

[AC-Vlan-interface100] quit

#ACL2000を設定し、サブネット192.168.1.0/24から通過するパケットだけを許可するルールを作成します。

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-acl-ipv4-basic-2000] quit

IPアドレスの取得にDHCPを使用するようにVLANインターフェイス200を設定します。

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address dhcp-alloc

インターフェイスVLANインターフェイス200でEasy IPを使用したアウトバウンドNATをイネーブルにします。

[AC-Vlan-interface200] nat outbound 2000

[AC-Vlan-interface200] quit

3. 次の手順に従って、ISPドメインを設定します。

extend-authという名前のISPドメインを作成します。

[AC] domain extend-auth

ACがポータルユーザーの認証、認可、またはアカウンティングを実行しないように設定します。

[AC-isp-extend-auth] authentication portal none

[AC-isp-extend-auth] authorization portal none

[AC-isp-extend-auth] accounting portal none

[AC-isp-extend-auth] quit

4. 電子メール認証を設定します。

ポータルWebサーバーwbsのURLとしてhttps://192.168.1.1/portalを指定します。

[AC] portal web-server wbs

[AC-portal-websvr-wbs] url https://192.168.1.1/portal

[AC-portal-websvr-wbs] quit

電子メール認証サーバーを作成します。

[AC] portal extend-auth-server mail

電子メール認証のプロトコルとしてPOP3およびIMAPを指定します。

[AC-portal-extend-auth-server-mail]mail-protocol pop3imap

[AC-portal-extend-auth-server-mail]quit

st1という名前のサービステンプレートを作成します。

[AC] wlan service-template st1

サービステンプレートst1を介してオンラインになるクライアントをVLAN100に割り当てます。

[AC-wlan-st-st1] vlan 100

サービステンプレートst1のSSIDをserviceに設定します。

[AC-wlan-st-st1] ssid service

サービステンプレートst1で直接ポータル認証を有効にします。

[AC-wlan-st-st1] portal enable method direct

電子メール認証の認証ドメインとして、ISPドメインの拡張認証を指定します。

[AC-wlan-st-st1] portal extend-auth domain extend-auth

サービステンプレートst1のポータルWebサーバーwbsを指定します。

[AC-wlan-st-st1] portal apply web-server wbs

サービステンプレートst1を有効にします。

[AC-wlan-st-st1] service-template enable

[AC-wlan-st-st1] quit

モデルWA4320i-CANでAP ap1を作成し、シリアルIDを210235A29G007C000020に設定します。

[AC] wlan ap ap1 model WA4320i-ACN

[AC-wlan-ap-ap1] serial-id 210235A29G007C000020

radio1のビューに入ります。

[AC-wlan-ap-ap1] radio 1

サービステンプレートst1をradio1にバインドします。

[AC-wlan-ap-ap1-radio-1] service-template st1

radio1を有効にします。

[AC-wlan-ap-ap1-radio-1] radio enable

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

HTTPSベースのローカルポータルWebサービスを作成し、そのビューに入ります。

[AC] portal local-web-server https

ローカルポータル認証用のデフォルトの認証ページファイルとして、ファイルdefaultfile.zipを指定します(ファイルがACのルートディレクトリに存在することを確認してください)。

[AC-portal-local-websvr-https] default-logon-page defaultfile.zip

[AC-portal-local-websvr-https] quit

宛先ベースのポータルフリー規則1および2を設定して、ポータルユーザーが認証無しにDNSにアクセスできるようにします。

[AC] portal free-rule 1 destination ip any udp 53

[AC] portal free-rule 2 destination ip any tcp 53

#(任意)client forwarding-location ap(ユーザーデータをCAPWAPトンネルを通さずに、

直接VLAN内を通す設定)の場合、以下のコマンドが必要。

[AC] portal host-check enable

設定の確認

#電子メール認証サーバーに関する情報を表示します。

[AC] display portal extend-auth-server mail Portal

extend-auth-server: mail

Mail protocol: POP3 IMAP

認証を渡す前に、ユーザーはポータル認証ページhttp://192.168.0.111/portalにのみアクセスできます。ユーザーからのすべてのWeb要求は、ポータル認証ページにリダイレクトされます。ユーザーがポータル認証ページの電子メール認証ボタンをクリックすると、ユーザーは電子メール認証ページにリダイレクトされます。電子メール認証を渡すと、ユーザーは他のネットワークリソースにアクセスできます。
http://192.168.0.111/portal

#すべてのポータルユーザーに関する情報を表示します。

[AC] display portal user all Total

portal users: 1

Username:

user AP name:

ap1 Radio ID: 1

SSID:service

Portal server: N/A

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0015-e9a6-7cfe	192.168.1.2	100	WLAN-BSS1/0/1

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A ACL

number/name: N/A

CAR: N/A

ポータルのトラブルシューティング

ユーザーに対してポータル認証ページがプッシュされない

症状

ユーザーがiMCポータル認証サーバーにリダイレクトされる場合、ポータル認証ページまたはエラーメッセージはユーザーに対して表示されません。ログインページは空白です。

解析

ポータルアクセスデバイスに設定されているキーとポータル認証サーバーに設定されているキーが矛盾しています。その結果、パケットの検証が失敗し、ポータル認証サーバーは認証ページの送信を拒否します。

解決策

ポータル認証サーバーにキーが設定されているかどうかを確認するには、アクセスデバイスのポータル認証サーバービューでこのコマンドを表示します。

- キーが設定されていない場合は、正しいキーを設定します。
- キーが設定されている場合は、ポータル認証サーバービューでipまたはipv6コマンドを使用してキーを修正するか、またはポータル認証サーバー上のアクセスデバイス用に設定されているキーを修正します。