Cisco AnyConnect セキュア モビリティ ソリューション ガイド

このマニュアルの構成は、次のとおりです。

Cisco AnyConnect セキュア モビリティの概要

ユーザとその所有デバイスは、オフィス、自宅、空港、カフェなど、さまざまな場所からインターネットに接続するため、さらにモバイル化が進んでいます。従来、ネットワーク内のユーザはセキュリティの脅威から保護されていましたが、ネットワーク境界外のユーザはアクセプタブル ユース ポリシーが適用されずにマルウェアからの保護も最小限であったため、現在よりもデータ損失のリスクが高くなっていました。

雇用主は、従業員やパートナーが場所やデバイスを問わずに作業できるフレキシブルな作業環境の創出を望んでいますが、同時に、企業の利益と資産をインターネット ベースの脅威から常時保護したいと考えています。

従来のネットワーク セキュリティ ソリューションやコンテンツ セキュリティ ソリューションは、ユーザと資産をネットワーク ファイアウォールで保護するには理想的でしたが、ユーザまたはデバイスがネットワークに接続していない場合や、セキュリティ ソリューションを介してデータがルーティングされない場合には効果がありません。

シスコは AnyConnect セキュア モビリティを提供することで、ネットワーク境界をリモート エンドポイントまで拡張し、Web セキュリティ アプライアンスによる Web フィルタリング サービスのシームレスな統合を実現します。Cisco AnyConnect セキュア モビリティを使用すると、革新的な新しい方法でコンピュータベースのプラットフォームやスマートフォン プラットフォーム上のモバイル ユーザを保護できます。エンド ユーザには、よりシームレスな常時保護されたエクスペリエンスが提供され、IT 管理者は包括的にポリシーを適用できるようになります。

インターネット上のリソースにアクセスして作業する必要があり、さまざまな種類のモバイル デバイスを使用して会社以外の場所で作業するユーザが存在する企業では、AnyConnect セキュア モビリティを使用すると役立ちます。

AnyConnect セキュア モビリティは、次のシスコ製品の機能の集まりです。

- Cisco IronPort Web セキュリティ アプライアンス（WSA）
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- Cisco AnyConnect クライアント

Cisco AnyConnect セキュア モビリティは、次の機能を提供してモバイル ワークフォースの課題に対処します。

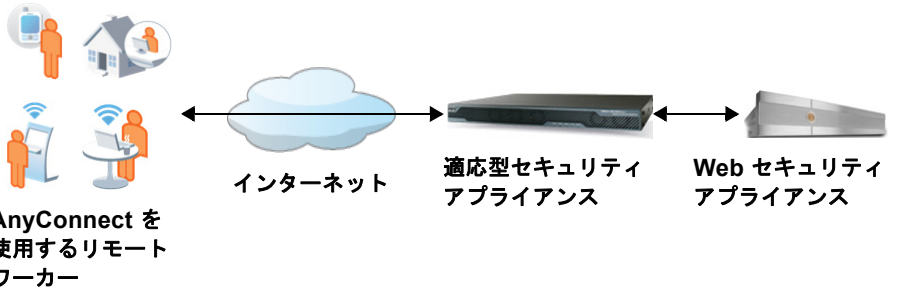
- **セキュアかつ持続的な接続：**（適応型セキュリティ アプライアンスをヘッドエンドに使用する）Cisco AnyConnect は、AnyConnect セキュア モビリティのリモート アクセス接続機能を提供します。ネットワークへのアクセスを許可する前に、ユーザとデバイスの両方を認証して検証する必要があるため、セキュアな接続が得られます。通常、AnyConnect はネットワーク間のローミング時も常時接続に設定されるため、接続は固定されます。AnyConnect は常時接続でありながら、十分な柔軟性も備えているため、ロケーションに応じてさまざまなポリシーを適用できます。また、インターネットにアクセスする前に契約条項に同意する必要がある「キャプティブ ポータル」で、ユーザのインターネット アクセスを許可します。

- **永続的なセキュリティとポリシーの適用**：Web セキュリティ アプライアンスは、アクセプタブル ユース ポリシーやマルウェアからの保護などのコンテキストに対応したポリシーを、モバイル（リモート）ユーザも含めたあらゆるユーザに適用します。また、Web セキュリティ アプライアンスは AnyConnect クライアントの認証に基づいて適応型セキュリティ アプライアンスからユーザ認証情報を受け取ることで、ユーザが Web コンテンツにアクセスするための自動認証手順を実現します。

AnyConnect セキュア モビリティの機能概要

Cisco AnyConnect セキュア モビリティは、制御とセキュリティをボーダレス ネットワークにまで拡張する、複数のシスコ製品の機能の集まりです。AnyConnect セキュア モビリティを提供するために連携する製品は、Web セキュリティ アプライアンス、適応型セキュリティ アプライアンス、Cisco AnyConnect クライアントです。

次の図に、これらのシスコ製品が連携して AnyConnect セキュア モビリティを提供する仕組みを示します。



リモート ユーザおよびモバイル ユーザは、Cisco AnyConnect Secure VPN クライアントを使用して適応型セキュリティ アプライアンスとの VPN セッションを確立します。適応型セキュリティ アプライアンスは、IP アドレスとユーザ名によるユーザの識別情報とともに、Web トラフィックを Web セキュリティ アプライアンスへ送信します。Web セキュリティ アプライアンスは、トラフィックをスキャンしてアクセプタブル ユース ポリシーを適用し、セキュリティ上の脅威からユーザを保護します。適応型セキュリティ アプライアンスは、安全と判断された、ユーザが受け入れ可能なすべてのトラフィックを戻します。

インターネット トラフィックのスキャンはすべて、モバイル デバイス上のクライアントではなく Web セキュリティ アプライアンスによって実行されます。そのため、モバイル デバイス（処理能力が制限されているものもある）に負担がかからず、全体的なパフォーマンスが改善されます。また、ネットワーク上のインターネット トラフィックをスキャンすることで、セキュリティ更新プログラムやアクセプタブル ユース ポリシーを簡単かつ迅速に更新できるため、クライアントへの更新のプッシュに何日、何週間、何ヵ月も待つ必要がありません。

Web セキュリティ アプライアンスは受信する要求を追跡し、リモート ユーザから受信したトラフィックに、リモート ユーザ用に設定されたポリシーを適用します。リモート ユーザの識別方法については、「ASA と WSA との間の通信」（P.4）を参照してください。

Web セキュリティ アプライアンスの設定方法によっては、AnyConnect クライアントが適応型セキュリティ アプライアンスとの VPN 接続を使用して、Web セキュリティ アプライアンスと直接通信する場合があります。詳細については、「クライアントからの通信」（P.5）を参照してください。

ASA と WSA との間の通信

Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスとインタラクションおよび通信を行うかどうかは、Web セキュリティ アプライアンスのリモート ユーザの識別設定によって決まります。Web セキュリティ アプライアンスは受信するトラフィックを追跡し、リモート ユーザから受信したトラフィックに、リモート ユーザ用に設定されたポリシーを適用します。次の方法のいずれかを使用して、リモート ユーザを識別します。

- **IP アドレスによる関連付け**：Web セキュリティ アプライアンス管理者は、リモート デバイスに割り当てられていると見なす IP アドレスの範囲を指定します。通常、適応型セキュリティ アプライアンスは、VPN 機能を使用して接続しているデバイスに、これらの IP アドレスを割り当てます。Web セキュリティ アプライアンスは、設定されているいずれかの IP アドレスからトランザクションを受信すると、そのユーザをリモート ユーザと見なします。この設定では、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスと通信しません。

- **Cisco ASA との統合：**Web セキュリティ アプライアンス管理者は、1 台以上の適応型セキュリティ アプライアンスと通信するように Web セキュリティ アプライアンスを設定します。適応型セキュリティ アプライアンスは、IP アドレスとユーザのマッピングを保持し、その情報を Web セキュリティ アプライアンスに伝達します。Web セキュリティ アプライアンスはトランザクションを受信すると、IP アドレスを取得して IP アドレスとユーザのマッピングをチェックし、ユーザ名を特定します。適応型セキュリティ アプライアンスと統合すると、リモート ユーザのシングル サインオンを有効にできます。この設定では、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスと通信します。

Web セキュリティ アプライアンスは、適応型セキュリティ アプライアンスと統合するように設定されると、初回起動時に、設定されているすべての適応型セキュリティ アプライアンスと HTTPS 接続を確立しようとします。接続が確立されると Web セキュリティ アプライアンスは、設定されている ASA アクセス パスワードを使用して適応型セキュリティ アプライアンスで認証します。認証が正常に行われると、適応型セキュリティ アプライアンスは Web セキュリティ アプライアンスに IP アドレスとユーザのマッピングを送信します。接続が開かれたまま、適応型セキュリティ アプライアンスは必要に応じて IP アドレスとユーザのマッピングを更新します。たとえば、新しい VPN 接続が確立されると新規ユーザがマッピングに追加され、VPN 接続が閉じられるとそのユーザがマッピングから削除されます。

（注） Web セキュリティ アプライアンスと適応型セキュリティ アプライアンスとの間の接続が失われた場合、Web セキュリティ アプライアンスはデフォルトで 60 秒ごとに接続の再確立を試みます。この時間間隔は、Web セキュリティ アプライアンスで設定できます。

クライアントからの通信

ユーザが Cisco AnyConnect を使用して VPN セッションを開始すると、AnyConnect クライアントは SSL を使用して適応型セキュリティ アプライアンスに接続します。クライアントは適応型セキュリティ アプライアンスで認証され、ネットワークの内部 IP アドレスが割り当てられます。

適応型セキュリティ アプライアンスと統合するように Web セキュリティ アプライアンスを設定している場合は、適応型セキュリティ アプライアンスがクライアントに、Web セキュリティ アプライアンスに直接通信して接続をテストするように指示します。クライアントと Web セキュリティ アプライアンスは、VPN セッションを使用して著作権ステータスなどの情報を交換します。

（注） クライアントは、架空のホストに要求を送信して Web セキュリティ アプライアンスへの接続を定期的にチェックします。デフォルトでは、架空のホストの URL は mus.cisco.com です。AnyConnect セキュア モビリティが有効になっている場合、Web セキュリティ アプライアンスは架空のホスト宛ての要求をインターセプトし、クライアントに応答します。

サポートされているアーキテクチャ

企業ネットワーク インフラは動的かつ固有なものであるため、AnyConnect セキュア モビリティ ソリューションの実装時にはさまざまなアーキテクチャについて考慮する必要があります。AnyConnect リモート アクセス接続に加えてセキュア モビリティを実装するための最小要件は、適応型セキュリティ アプライアンス、Web セキュリティ アプライアンス、および多くの場合 WCCP（Web キャッシュ通信プロトコル）が有効になっているルータから構成されます。ただし、追加のアプライアンスやルータを含めるため、これらのアーキテクチャを拡張できるようにする設計上の要件があります。

WCCP ルータにより、ネットワークは Web トラフィックを WSA へ透過的にリダイレクトして、クライアント アプリケーションがネットワーク上のプロキシ サーバの存在を認識しないようにすることができます。このマニュアルに記載されているほとんどのアーキテクチャには、少なくとも 1 台の WCCP ルータが必要です。適応型セキュリティ アプライアンスにおける WCCP 実装制限により、これらのケースのほとんどで WCCP ルータが必要となります。

（注） AnyConnect セキュア モビリティ用にネットワークを設定する場合は、自社に必要な適応型セキュリティ アプライアンスの機能要件をすべて考慮してください。たとえば、適応型セキュリティ アプライアンスが配置されているネットワーク内の場所によっては、IPS などの一部の機能が機能する場合と機能しない場合があります。

表 5-1 に、ネットワークで AnyConnect セキュア モビリティを展開する場合に考慮すべきアーキテクチャ例を示します。

表 5-1　　アーキテクチャ シナリオの概要

アーキテクチャ シナリオ	説明
「アーキテクチャ シナリオ 1：単一サブネット」（P.8）	このアーキテクチャには次のような特長があります。 • Web トランザクションは Web セキュリティ アプライアンスへ透過的にリダイレクトされ、それらのトランザクションは WCCP 対応ルータによってリダイレクトされます。 • 適応型セキュリティ アプライアンス、WCCP ルータ、Web セキュリティ アプライアンスは、同じサブネット上に配置されます。
「アーキテクチャ シナリオ 2：複数サブネット」（P.10）	このアーキテクチャは「アーキテクチャ シナリオ 1：単一サブネット」に似ていますが、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスや WCCP ルータと異なるサブネット上に配置される点が異なります。
「アーキテクチャ シナリオ 3：明示的な転送プロキシ」（P.12）	このアーキテクチャは「アーキテクチャ シナリオ 1：単一サブネット」に似ていますが、Web トラフィックを Web プロキシとして Web セキュリティ アプライアンスへ明示的に転送するようにクライアント アプリケーションが設定されている点が異なります。WCCP 対応ルータは必要ありません。
「アーキテクチャ シナリオ 4：WCCP 非対応のルータ」（P.14）	このアーキテクチャではルータを使用しますが、WCCP 対応ルータは使用されません。代わりに ASA（WCCP 対応）が WCCP を使用して、Web トラフィックを WSA にリダイレクトします。WCCP 対応ルータがない場合は、このアーキテクチャを使用します。

アーキテクチャ シナリオ 1：単一サブネット

図 1 は、この項で説明するアーキテクチャを示しています。

図 1　　単一サイトと単一サブネット

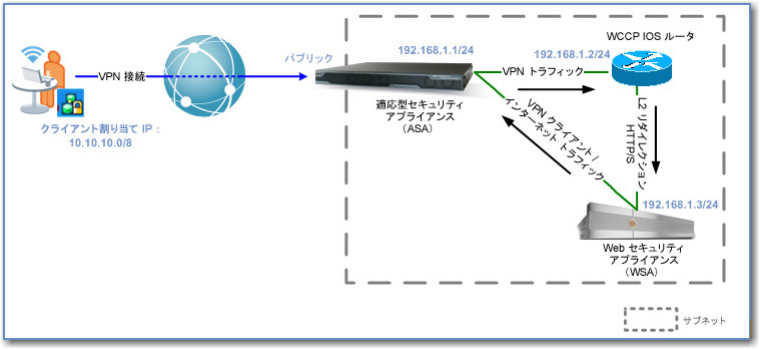


図 1 の展開シナリオは、リモート アクセスおよびインターネット ゲートウェイとして機能する ASA が含まれたレイヤ 2（L2）トポロジを表しています。また、このトポロジには、Web トラフィックの L2 リダイレクション用 WCCP ルータも含まれます。以下のコマンド例はすべて、図 1 の例を示しています。この展開シナリオのトラフィック フローは、次のように構成されます。

- AnyConnect クライアントは ASA ヘッドエンドとの SSL VPN セッションを確立し、そのセッションを介してすべてのトラフィックを転送します。セキュリティ管理者が、特定のトラフィックを VPN セッションから排除する VPN ポリシーを定義する場合もあります。たとえば、接続されているエンドユーザのためにローカル印刷を有効にすることがあります。
- ASA には、すべての VPN トラフィックをトンネルから WCCP ルータ（`192.168.1.2/24`）に転送するトンネル デフォルト ゲートウェイ（`route inside 0.0.0.0 0.0.0.0 192.168.1.2 255.255.255.0 Tunneled`）が設定されます。

- WCCP ルータは Web トラフィックだけを WSA に転送します。インターネットに向かう非 Web トラフィックをすべてデフォルト ルート（`ip route 0.0.0.0 0.0.0.0 192.168.1.1`）、この場合は ASA に転送するか、宛先が企業ネットワークの場合は事前定義されたスタティック ルートに転送します。WCCP ルータでは、コマンド構文（`ip wccp [port] redirect out` ではなく）`ip wccp [port] redirect in` を、L2 リダイレクション用に設定されたインターフェイスに適用する必要があります。このコマンドによって、インターフェイスへの着信 Web トラフィックが WSA へ正常にリダイレクトされるようになります。
- WSA は WCCP ルータからリダイレクトされた Web トラフィックを受信し、そのポリシーを AnyConnect クライアントから受信したトラフィックに適用します。Web 要求へのアクセスを許可する場合は、トラフィックを書き換えてからデフォルト ルート（ASA）を介してインターネットに転送します。これによって、ASA はスキャンとポリシー適用のためにトラフィックを WSA へ戻せるようになります。正常にスキャンされたトラフィックを AnyConnect クライアントへ戻すルートが WSA にあることを確認してください。たとえば、スタティック ルートを WSA に追加して、クライアント IP アドレス プール（`10.10.10.0/8`）宛てのすべてのトラフィックを ASA に戻すことができます。

（注） インターネットから ASA に戻された非 Web トラフィックは、そのトラフィックの送信元と宛先が AnyConnect クライアント IP アドレス プール（`10.10.10.0/8`）に含まれているとドロップされます。これを回避するため、ASA にスタティック ルート（`route inside 10.10.10.0 255.0.0.0 192.168.1.2`）を設定し、AnyConnect クライアント IP アドレス プールにトラフィックを転送できるようにします。

セキュア モビリティのコンポーネントはすべてフラット ネットワーク上に配置し、WCCP ルータが総称ルーティング カプセル化（GRE）ではなくレイヤ 2 リダイレクションを使用できるようにします。GRE はトラフィック オーバーヘッドを追加してレイヤ 3 で動作し、WCCP ルータと WSA が異なるサブネット上にある場合に必要です。

図 1（P.8）のように ASA がリモート アクセスとインターネット ゲートウェイの両方として機能する場合は、ネットワーク アドレス変換（NAT）またはポート アドレス変換（PAT）を ASA 上に設定し、非 Web トラフィックやプライベート IP アドレス空間からのトラフィックをインターネットにルーティングする必要があります。また、企業ネットワークから AnyConnect クライアントに戻されたトラフィックが NAT コマンドや PAT コマンドの影響を受けないように、定義されている AnyConnect クライアント IP アドレス プールに対して NAT 免除ルールを設定する必要があります。

アーキテクチャ シナリオ 2：複数サブネット

図 2 は、この項で説明するアーキテクチャを示しています。

図 2　　単一サイトと複数サブネット

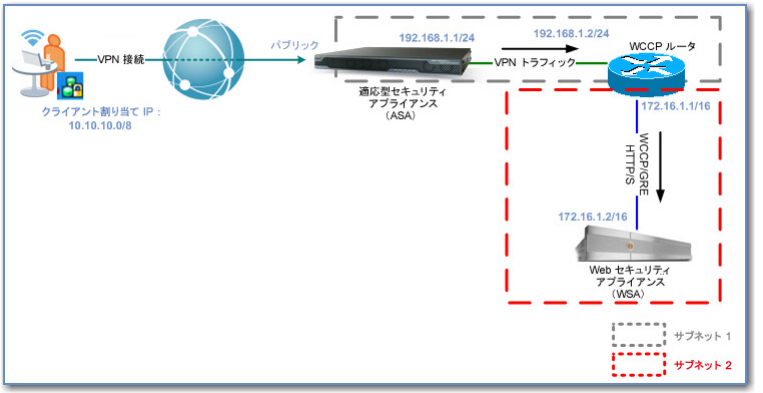


図 2 の展開シナリオは、図 1（P.8）に似たアーキテクチャを表しています。ただし、このアーキテクチャでは、WSA が WCCP ルータとは別のサブネット上にある場合に必要な総称ルーティング カプセル化（GRE）リダイレクションを使用して WCCP が導入されます。図 1 に示されたアーキテクチャのように、トラフィック フローは基本的に同じです。ただし、リダイレクション方法として GRE を含んだレイヤ 3（L3）を考慮する必要があります。また、トラフィックを ASA に戻すため、WSA 上に代替のルーティング エントリを設定することを検討してください。

ネットワーク トポロジのために WSA を WCCP ルータと同じサブネット上に配置できない場合や、すべての Web トラフィックを別のネットワーク トラフィックとして異なるサブネットから WCCP ルータに取り込む場合は、図 1 ではなく図 2 のアーキテクチャを使用します。インターネットに向かうトラフィックをこのように分離すると、ネットワーク管理者は Web トラフィックの監視とレポートの作成をより簡単に実行できるようになります。また、トラフィックが WSA Web プロキシを通過しない場合は、すべてのユーザからの Web トラフィックをブロックするファイアウォール ポリシーを作成できます。

WCCP ルータは、リダイレクション方法を WSA と自動的にネゴシエートして GRE ヘッダー内に Web トラフィックをカプセル化し、それをルーティング テーブルに基づいて WSA にルーティングします。インターネットに向かう非 Web トラフィックは、デフォルト ルート（`ip route 0.0.0.0 0.0.0.0 192.168.1.1`）、この場合は ASA に転送されるか、宛先が企業ネットワークの場合は事前定義されたスタティック ルートに転送されます。WCCP ルータでは、コマンド構文 `ip wccp [port] redirect in` を、リダイレクション用に設定されたインターフェイスに適用する必要があります。このコマンドによって、インターフェイスへの着信 Web トラフィックが WSA へリダイレクトされるようになります。WSA は GRE パケットをカプセル化し、そのセキュリティ ポリシーを適用します。

図 1（P.8）のアーキテクチャのように、スキャンされたトラフィックを AnyConnect クライアントにへ戻すため、ASA への適切なルート（`route 10.10.10.0/8 x.x.x.x`）を指定して WSA を設定する必要があります。この場合のルータは、通常、ルーティング インフラストラクチャのディストリビューション レイヤまたはアグリゲーション レイヤに配置されます。

アーキテクチャ シナリオ 3：明示的な転送プロキシ

図 3 は、この項で説明するアーキテクチャを示しています。

図 3　　明示的なモード ポリシーの適用

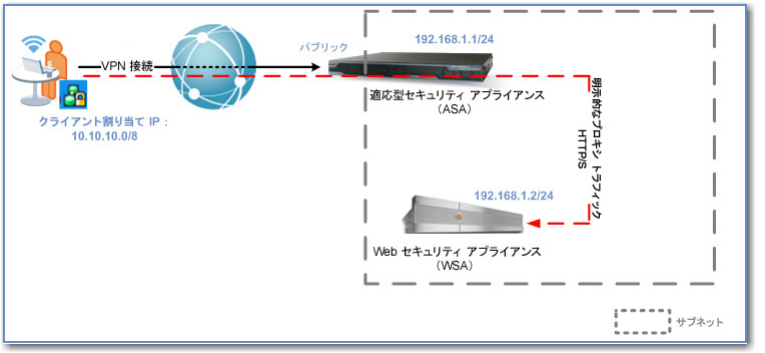


図 3 に示された展開シナリオでは、WSA へ透過的にリダイレクトされる Web トラフィックではなく、Web トラフィック用に WSA を明示的に使用するように、クライアント Web トラフィックが設定されています。Web ブラウザなどのクライアント アプリケーションは、プロキシ サーバとして WSA を明示的に使用するように設定されます（`address: 192.168.1.2, port: 80/443`）。これは、WCCP ルータが Web トラフィックを WSA へ透過的にリダイレクトし、クライアントは Web トラフィックがプロキシ サーバを通過することを認識しない展開（図 1 と図 2）とは異なります。

（注） ブラウザのプロキシ設定は、エンド ユーザが手動で定義することも、VPN の確立時に ASA によって動的に定義することも可能です。Adaptive Security Device Manager（ASDM）を使用するとダイナミック プロキシ コンフィギュレーションを設定できます。これには、ASA の定義済み内部グループ ポリシーで、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [*グループ名*] > [Edit] > [Advanced] > [Browser Proxy] の順に選択します。

Web トラフィックと非 Web トラフィックはどちらも VPN セッションを介して ASA に転送されます。ただし、Web トラフィックは、ブラウザのプロキシ設定で定義されているように WSA へ明示的に送信され、非 Web トラフィックは、ASA のルーティング テーブルに基づいてルーティングされます。

（注） ASA を使用したプロキシ コンフィギュレーションの設定は、（AnyConnect クライアントに接続された）Windows 上の Internet Explorer と Mac OS 上の Safari に対してのみ動的に展開できます。その他のブラウザは、WSA をプロキシとして明示的に使用する場合、クライアント マシン上で手動設定する必要があります。Web トラフィックを WSA へ透過的にリダイレクトするとエンド ユーザのユーザ エクスペリエンスは向上しますが、WSA を使用するようにクライアント ブラウザを明示的に設定すると、AnyConnect クライアントが VPN セッションから WSA へ Web トラフィックを正常にルーティングできる場合に、あらゆるネットワーク アーキテクチャで展開できます。

ユーザがリモートで、Web トラフィック用に WSA を明示的に使用するようにクライアント アプリケーションが設定されている場合は、プロキシ サーバを使用するようにクライアント アプリケーションを設定する際、次の情報を考慮します。

- **VPN 接続が確立される前に使用されるプロキシ設定：**プロキシを使用するように Internet Explorer が設定されていると、AnyConnect は ASA への接続にそれらのプロキシ設定を使用します。ただし、これらのプロキシ設定がエンタープライズ LAN 内の WSA をポイントしている場合、AnyConnect は ASA への接続に失敗します。これを回避するには、次の作業のいずれかを行う必要があります。
  - ASA の例外を追加するように、ブラウザのプロキシ設定を変更する。
  - AnyConnect プロファイルを使用して、ProxySettings 属性を IgnoreProxy に設定する。詳細については、「ProxySettings 属性の設定」（P.14）を参照してください。
- **VPN 接続が確立された後に使用されるプロキシ設定：**Web トラフィックが必ず WSA へ送信されるようにするには、次の 2 つの選択肢があります。
  - 現在のブラウザのプロキシ設定を保持する（上記で推奨されているように ASA は例外）。
  - ASDM を使用して、ブラウザでプロキシ設定を動的に設定する。

ProxySettings 属性の設定

AnyConnect プロファイルの ProxySettings 属性を IgnoreProxy に設定するには、ASDM を使用します。『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「Configuring AnyConnect Features」の章の「Configuring the Client to Ignore Browser Proxy Settings」の項に記載されている説明に従ってください。

シスコ製品のマニュアルへのアクセス方法については、「その他のマニュアル」（P.22）を参照してください。

（注） IgnoreProxy などの AnyConnect プロファイル設定は、AnyConnect クライアントが ASA に接続する場合にのみ適用されます。ASA とのトンネルの確立後、クライアントはこれらの設定を使用しません。

アーキテクチャ シナリオ 4：WCCP 非対応のルータ

図 4 は、この項で説明するアーキテクチャを示しています。

図 4　　ASA での WCCP の使用方法

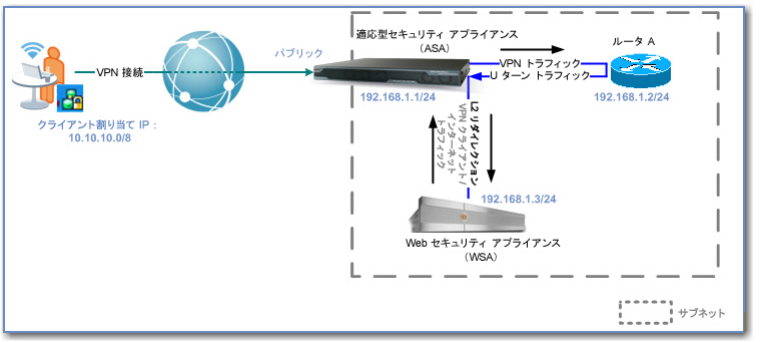


図 4 の展開シナリオは、WCCP ルータを使用してトラフィックをリダイレクトする代わりに、ASA で WCCP を使用して Web トラフィックを WSA にリダイレクトする方法を示しています。前述の展開シナリオでは、WCCP ルータを使用して Web トラフィックを WSA へ透過的にリダイレクトしています。WCCP 対応ルータがない場合は、このアーキテクチャを使用します。代わりに ASA の WCCP 機能を使用して、Web トラフィックを WSA にリダイレクトできます。この展開シナリオでは、あらゆるルータを使用できます。

図 4 の展開シナリオでは、ASA はすべての VPN トラフィックをそのトンネル デフォルト ゲートウェイ、つまりルータ A（`route inside 0.0.0.0 0.0.0.0 192.168.1.2 255.255.255.0 Tunneled`）に転送します。ルータ A は VPN Web トラフィックを ASA（`ip route 0.0.0.0 0.0.0.0 192.168.1.1`）に戻し、非 Web トラフィックをルーティング テーブルに基づいて転送します。次に、ASA は、スキャンのために WCCP を使用して Web トラフィックを WSA にリダイレクトします。

前述したアーキテクチャのように、インターネット ゲートウェイへのデフォルト ルートを WSA に設定し、そのポリシーを適用する必要があります。また、WSA に ASA へ戻すルート（`route 10.10.10.0/8 192.168.1.1`）を設定し、スキャンされたトラフィックを AnyConnect クライアントへ戻す必要があります。

（注） WCCP に対応した同じインターフェイスで ASA にトラフィックを取り込む場合、ASA バージョン 8.3 では、WCCP のみを使用して Web トラフィックをリダイレクトできます。ただし、AnyConnect クライアント トラフィックは、WCCP に対応した同じインターフェイス（WSA に接続されている同じインターフェイス）で ASA に取り込まれません。この問題に対処するには、WCCP 対応インターフェイスを使用しないでルータを接続し、すべてのトラフィックをそのルータに転送して、それを WCCP 対応インターフェイスで ASA に戻す必要があります。これにより、ASA は WCCP を使用して Web トラフィックを WSA にリダイレクトし、スキャンできるようになります。図 4 では、ルータ A は WSA と同じインターフェイス（内部インターフェイス）で、すべてのトラフィックを ASA に戻しています。

AnyConnect セキュア モビリティの設定

VPN を使用してネットワークに接続しているユーザのセキュア モビリティを実現するには、次の製品を設定する必要があります。

- **Cisco IronPort Web セキュリティ アプライアンス**：詳細については、「AnyConnect セキュア モビリティの WSA サポートの設定」（P.16）を参照してください。
- **Cisco 適応型セキュリティ アプライアンス**：詳細については、「AnyConnect セキュア モビリティの ASA サポートの設定」（P.18）を参照してください。
- **Cisco AnyConnect セキュア モビリティ クライアント**：詳細については、「AnyConnect セキュア モビリティの AnyConnect サポートの設定」（P.19）を参照してください。

Web セキュリティ アプライアンスと適応型セキュリティ アプライアンスを統合するには、次の情報が必要です。

- 個々の適応型セキュリティ アプライアンスの IP アドレス
- 個々の適応型セキュリティ アプライアンスのポート番号
- 個々の Web セキュリティ アプライアンスの IP アドレス
- 個々の Web セキュリティ アプライアンスのポート番号
- 個々の適応型セキュリティ アプライアンスおよび Web セキュリティ アプライアンスで設定する単一のアクセス パスワード

セキュア モビリティを使用するには、次のバージョンのシスコ製品を使用する必要があります。

- Cisco 適応型セキュリティ アプライアンス Release 8.3.1.6 以降
- Cisco Adaptive Security Device Manager（ASDM）Release 6.3 以降
- Cisco IronPort Web セキュリティ アプライアンス Version 7.0 以降

AnyConnect セキュア モビリティの WSA サポートの設定

Web セキュリティ アプライアンス で AnyConnect セキュア モビリティが有効な場合は、リモート ユーザとローカル ユーザを区別して、リモート ユーザとローカル ユーザに別々のポリシーを作成できます。たとえば、ユーザが社外にいる（リモート ユーザの）場合はアート サイトやエンタテインメント サイトへのアクセスを許可し、ユーザが社内にいる（ローカル ユーザの）場合はアクセスをブロックするアクセス ポリシーを作成できます。

AsyncOS for Web Version 7.0 以降は AnyConnect セキュア モビリティをサポートしています。

AnyConnect セキュア モビリティと連動するように Web セキュリティ アプライアンスを設定するには、次の作業を実行します。

1. **Web セキュリティ アプライアンスで AnyConnect セキュア モビリティ機能を有効にします。**[Security Services] > [Mobile User Security] ページで、この機能を有効にします。AnyConnect セキュア モビリティ 機能を有効にする際、特定の IP アドレスに関連付けるか、Cisco 適応型セキュリティ アプライアンスと統合することで、リモート ユーザの識別方法を選択します。IP アドレスでユーザが識別される場合は、Web セキュリティ アプライアンスは適応型セキュリティ アプライアンスと通信しません。

（注） 1 つのクラスタに複数の適応型セキュリティ アプライアンスが設定されている場合は、そのクラスタの個々の適応型セキュリティ アプライアンスと通信するように Web セキュリティ アプライアンスを設定します。ハイ アベイラビリティのために 2 台の適応型セキュリティ アプライアンスが設定されている場合は、アクティブな適応型セキュリティ アプライアンスに限って通信するように Web セキュリティ アプライアンスを設定します。

2. **リモート ユーザに適用するアイデンティティ ポリシーを 1 つ以上作成します。** アイデンティティに認証が必要か否かを選択できます。
   - **[No authentication required]**：認証を使用しないようにアイデンティティを設定します。ユーザは IP アドレスで識別されます。
   - **[Authentication required]**：リモート ユーザにのみ適用し、Cisco 適応型セキュリティ アプライアンスと統合することでユーザを透過的に識別するように、アイデンティティを設定します。ユーザは、適応型セキュリティ アプライアンスからの IP アドレスとユーザ名のマッピングを使用して、ユーザ名で識別されます。
3. **リモート ユーザ用に設定されたアイデンティティを使用する他のポリシーを作成します。** 設定はすべて、ビジネス ニーズに応じて設定します。AnyConnect セキュア モビリティに特定のポリシー設定は必要ありません。

AnyConnect セキュア モビリティの有効化とリモート ユーザの操作の詳細については、バージョン 7.0 以降の『*IronPort AsyncOS for Web User Guide*』の「Achieving Secure Mobility」の章を参照してください。Web セキュリティ アプライアンスの Web インターフェイスから、オンライン ヘルプの『*IronPort AsyncOS for Web User Guide*』にアクセスできます。また、cisco.com の『*IronPort AsyncOS for Web User Guide*』にもアクセス可能です。シスコ製品のマニュアルへのアクセス方法については、「その他のマニュアル」（P.22）を参照してください。

AnyConnect セキュア モビリティが有効になり、リモート ユーザ用のポリシーが作成されると、Web セキュリティ アプライアンスでリモート トラフィックに関するレポートを表示できるようになります。

AnyConnect セキュア モビリティの ASA サポートの設定

適応型セキュリティ アプライアンスで AnyConnect セキュア モビリティを有効にするには、Web セキュリティ アプライアンスにアクセスするための情報が必要です。適応型セキュリティ アプライアンスと Web セキュリティ アプライアンスが相互に通信するように設定されると、適応型セキュリティ アプライアンスはスキャンのために、AnyConnect セキュア モビリティ クライアントから Web セキュリティ アプライアンスへトラフィックを送信できるようになります。クライアントは定期的にチェックして、Web セキュリティ アプライアンスの保護が有効であることを確認します。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Mobile User Security] の順に選択し、[Mobile User Security (MUS)] ダイアログ ボックスを使用して AnyConnect セキュア モビリティを有効にします。

AnyConnect セキュア モビリティをサポートするように適応型セキュリティ アプライアンスを設定するには、次の作業を実行します。

1. 適応型セキュリティ アプライアンスをリリース 8.3.1.6 以降にアップグレードします。
2. ASDM をリリース 6.3 以降にアップグレードします。
3. ASDM の [Mobile User Security] ウィンドウで、適応型セキュリティ アプライアンスが通信する Web セキュリティ アプライアンスを 1 台以上追加します。[Add] または [Edit] を選択したら、インターフェイス名、IP アドレス、ホストのマスクを指定できます。
4. 適応型セキュリティ アプライアンスで、モバイル ユーザ セキュリティ機能を有効にします。これによって、適応型セキュリティ アプライアンスは、シングル サインオン機能のためにユーザ クレデンシャルを Web セキュリティ アプライアンスへ渡すセキュアな HTTPS 接続を使用して、Web セキュリティ アプライアンスと通信できるようになります。有効にした場合は、適応型セキュリティ アプライアンスにコンタクトする際、Web セキュリティ アプライアンスによって使用されるアクセス パスワードを入力する必要があります。また、使用するサービスのポート番号も入力する必要があります。Web セキュリティ アプライアンスが存在しない場合、ステータスは disabled になります。
5. パスワードを変更します。適応型セキュリティ アプライアンスと Web セキュリティ アプライアンスとの間の認証に必要な Web セキュリティ アプライアンスアクセス パスワードを設定および変更できます。このパスワードは、Web セキュリティ アプライアンスに設定されている当該パスワードと一致する必要があります。

6. （オプション）適応型セキュリティ アプライアンスに接続されている Web セキュリティ アプライアンスのセッション情報と接続時間を表示します。

適応型セキュリティ アプライアンスの設定の詳細については、マニュアルを参照してください。マニュアルの場所については、「その他のマニュアル」（P.22）を参照してください。

AnyConnect セキュア モビリティの AnyConnect サポートの設定

AnyConnect クライアントで AnyConnect セキュア モビリティを使用すると、ユーザはセキュリティ上の脅威から簡単かつシームレスに保護され、ユーザの Web トランザクションに、IT 管理者が設定したアクセプタブル ユース ポリシーが適用されます。AnyConnect セキュア モビリティが有効な AnyConnect クライアントでステータス メッセージを確認しなければ、通常、AnyConnect クライアント ユーザは、トラフィックが Web セキュリティ アプライアンスによってスキャンされていることに気づきません。

AnyConnect クライアントが AnyConnect セキュア モビリティと連動できるようにするには、次の作業を実行します。

1. 適応型セキュリティ アプライアンスをリリース 8.3.1.6 以降にアップグレードします。
2. ASDM をリリース 6.3 以降にアップグレードします。
3. AnyConnect セキュア モビリティ クライアント パッケージ Release 2.5 以降を、適応型セキュリティ アプライアンスにロードします。
4. ASDM を使用して、通常どおりネットワーク（クライアント）アクセスをサポートするように、適応型セキュリティ アプライアンスを設定します。
5. ASDM で、VPN プロファイルを常時接続に設定します。ユーザが非信頼ネットワーク内にいる場合は、この機能を設定すると便利です。VPN プロファイルを常時接続に設定する場合は、Trusted Network Detection（TND）を有効にする必要もあります。

   常時接続機能によりユーザがコンピュータにログオンすると、AnyConnect は VPN セッションを自動的に確立します。VPN セッションは、ユーザがコンピュータからログオフするまで維持されます。物理的な接続が失われてもセッションは維持され、AnyConnect は、適応型セキュリティ アプライアンスとの物理的な接続の再確立を絶えず試行し、VPN セッションを再開します。

TND を使用すると、ユーザが企業ネットワーク（信頼ネットワーク）内にいる場合は自動的に AnyConnect が VPN 接続を解除し、企業ネットワークの外（非信頼ネットワーク）にいる場合は VPN 接続を開始するように設定できます。

6. 常時接続 VPN を設定すると、モバイル ユーザのエクスペリエンスに影響する次のオプションを任意に有効化できます。

   - **[Connect Failure Policy]**：AnyConnect が常時接続機能に従って VPN セッションを開始または維持しようとして失敗すると、trusted として設定されていないサービスやドメインを使用してユーザがネットワーク接続を確立できるかどうか、接続障害ポリシーによって判断されます。VPN プロファイルをフェール オープンまたはフェール クローズに設定できます。
   - **[Allow Captive Portal Remediation]**：これは、ネットワーク アクセスを取得するため、キャプティブ ポータルのホット スポット要件を満たすプロセスです。インターネット アクセスを提供する機能によって、アクセス権を取得する前に条件を受け入れるように要求されると、ユーザはキャプティブ ポータル環境に入ります。デフォルトでは、キャプティブ ポータルによって AnyConnect が VPN に接続しないように制御されます。ユーザがアクセス権を取得する条件を満たせるように数分間待機してから AnyConnect が VPN に接続できるようにするには、[Allow Captive Portal Remediation] を有効にする必要があります。
   - **[Apply Last VPN Local Resource Rules]**：[Connect Failure Policy] がフェール クローズに設定されていると、この機能によってユーザはローカル印刷やテザー デバイスの同期化を実行できるようになります。これには、適切なファイアウォール ルールを設定する必要もあります。

Cisco AnyConnect セキュア モビリティ クライアントの設定の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。マニュアルの場所については、「その他のマニュアル」（P.22）を参照してください。

トラブルシューティング

Web セキュリティ アプライアンス：

- AnyConnect セキュア モビリティのイベントは、User Discovery Service（UDS）ログに保存されます。
- Web セキュリティ アプライアンスの Web インターフェイスには、設定されている適応型セキュリティ アプライアンスへの接続をテストするボタンが用意されています。
- `musstatus` CLI コマンドを使用して、適応型セキュリティ アプライアンスと Web セキュリティ アプライアンスの接続と統計情報を表示します。

適応型セキュリティ アプライアンス：

- `mus server enable <port>` コマンドは、`show config | include mus` を使用して検証できます。
- `debug webvpn mus <1-255>` は、その他の AnyConnect セキュア モビリティ デバッグ情報を有効にします。
- ログは syslog を使用して取得できます。

ASDM：

- `[Monitoring] -> [VPN] -> [WSA Sessions]` の順に選択すると、ホストと稼動時間の統計情報が表示されます。

AnyConnect セキュア モビリティ クライアント：

- DART は、エンドポイント イベント ログ、インストール ログ、システム情報、ダンプ ファイル、プロファイル、プリファレンスなどを収集します。
- zip ファイルを作成します。
- 適応型セキュリティ アプライアンスから、またはスタンドアロン インストーラを使用して動的にインストールできます。
- [Start] メニューから、または [Troubleshoot] ボタンを使用してクライアントから起動できます。

その他のマニュアル

このマニュアルは、AnyConnect セキュア モビリティ ソリューション全体の概要を示すことを目的としています。製品の各コンポーネントの詳細な設定手順は記載されておらず、各コンポーネントの他の機能との潜在的な相互作用をすべて示した一覧もありません。このソリューションの各コンポーネントをインストール、設定、アップグレードする方法の詳細については、各製品のリリース ノートとユーザ ガイドを参照してください。

Cisco 適応型セキュリティ アプライアンス（ASA）のマニュアル ホームページ：

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

Cisco AnyConnect のマニュアル ホームページ：

http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco AnyConnect セキュア モビリティ クライアントのマニュアル ホームページ:

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html

Cisco Adaptive Security Device Manager（ASDM）のマニュアル ホームページ：

http://www.cisco.com/en/US/products/ps6121/products_installation_and_configuration_guides_list.html

Cisco IronPort Web セキュリティ アプライアンスのマニュアル ホームページ：

http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html

Cisco AnyConnect セキュア モビリティ ソリューションの概要：

http://www.cisco.com/en/US/netsol/ns1049/index.html

サポートへの問い合わせ

Cisco AnyConnect セキュア モビリティ ソリューションは複数のシスコ製品をカバーしているため、AnyConnect セキュア モビリティ関連の問題を解決するために支援を得る際、別のサポート グループに問い合わせる必要が生じる場合があります。各 AnyConnect セキュア モビリティ製品のサポートは、Cisco TAC（Technical Assistance Center）または IronPort カスタマー サポートのさまざまな製品サポート チームが担当しています。

Cisco TAC と Cisco IronPort カスタマー サポートは、相互に協力し合って AnyConnect セキュア モビリティ関連の問題を解決するためのコミュニケーション手段を持っていますが、AnyConnect セキュア モビリティに関する問題に遭遇した場合は、自ら最善の判断を下して問題の所在を特定し、可能な場合は適切なサポート チームに問い合わせてください。これによって、問題解決に必要な時間が短縮されます。

- 適応型セキュリティ アプライアンスまたは AnyConnect クライアント関連の問題については、次の URL にある Cisco TAC でケースを開いてください。`http://tools.cisco.com/ServiceRequestTool/create/launch.do` テクノロジー分野は [Security - Adaptive Security Appliance (ASA) and PIX] を使用し、サブテクノロジー分野は [WebVPN/SSLVPN - Anyconnect Client issue] を使用します。
- Web セキュリティ アプライアンス関連の問題については、Web セキュリティ アプライアンスのビルトイン サポート要求機能を使用して、Cisco IronPort カスタマー サポートでケースを開いてください。CLI から `supportrequest` コマンドを使用するか、Web インターフェイスから [Support and Help] > [Open A Support Case] の順に進みます。あるいは、次の URL にある Web ページからケースを開くことができます。`http://www.cisco.com/web/ironport/index.html`

現在問題が発生している AnyConnect セキュア モビリティ製品を特定するには、「トラブルシューティング」（P.21）に記載されているトラブルシューティングのヒントを活用すると便利です。特に、次のアプローチを検討してください。

- 以前にそのソリューションで作業した場合は、最後に変更された部分を調査します。
- デバイス間の基本的なネットワーク接続をテストします。たとえば、クライアントから適応型セキュリティ アプライアンス、適応型セキュリティ アプライアンスからルータ、ルータから Web セキュリティ アプライアンスへの ping を実行し、ping が失敗した接続間を特定します。
- エラー メッセージや警告メッセージについては、適応型セキュリティ アプライアンスの syslog メッセージを確認します。