リモート アクセス

サービス ディスカバリ要件のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	サービス ディスカバリ要件，（1 ページ）	
ステップ 2	DNS の要件，（2 ページ）	
ステップ 3	証明書の要件，（2 ページ）	
ステップ 4	_collab-edge SRV レコードのテスト，（2 ページ）	

サービス ディスカバリ要件

サービス ディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。Expressway for Mobile and Remote Access により、企業ネットワークのサービスにアクセスできます。クライアントが Expressway for Mobile and Remote Access 経由で接続し、サービスを検出できるようにするには、以下の要件を満たす必要があります。

- DNS の要件
- 証明書の要件
- 外部 SRV `_collab-edge` をテストします。

DNS の要件

リモート アクセスによるサービス ディスカバリの DNS 要件は次のとおりです。

- 外部 DNS サーバ上で _collab-edge DNS SRV レコードを設定します。
- 内部ネーム サーバ上で _cisco-uds DNS SRV レコードを設定します。
- オプションで、IM and Presence サーバのドメインが音声サーバのドメインと異なるハイブリッド クラウド ベース アーキテクチャを展開する場合、_collab-edge レコードを含む DNS サーバを検出するための音声サービス ドメインを設定するようにします。

証明書の要件

リモート アクセスを設定する前に、Cisco VCS Expressway と Cisco Expressway-E のサーバ証明書をダウンロードします。このサーバ証明書は、HTTP と XMPP の両方に使用されます。

Cisco VCS Expressway 証明書の設定の詳細については、『Configuring Certificates on Cisco VCS Expressway』を参照してください。

_collab-edge SRV レコードのテスト

SRV レコードのテスト

SRV レコードの作成後にテストして、それらが動作するかどうかを確認します。

手順

ステップ 1 コマンド プロンプトを開きます。

ステップ 2 nslookup と入力します。
デフォルトの DNS サーバとアドレスが表示されます。これが想定された DNS サーバであることを確認します。

ステップ 3 set type=SRV と入力します。

ステップ 4 それぞれの SRV レコードの名前を入力します。
例：`_cisco-uds.exampledomain`

- サーバとアドレスが表示される：SRV レコードにアクセスできます。
- `_cisco-uds.exampledomain: Non-existent domain`：SRV レコードに問題があります。

Cisco AnyConnect の展開ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション プロファイル, （3 ページ）	
ステップ 2	VPN 接続の自動化, （4 ページ）	
ステップ 3	AnyConnect マニュアル リファレンス, （8 ページ）	
ステップ 4	セッション パラメータ, （8 ページ）	

Cisco AnyConnect の導入

アプリケーション プロファイル

Cisco AnyConnect セキュア モビリティ クライアントをデバイスにダウンロードした後で、ASA はこのアプリケーションに対してコンフィギュレーション プロファイルをプロビジョニングする必要があります。

Cisco AnyConnect セキュア モビリティ クライアントのコンフィギュレーション プロファイルには、会社の ASA VPN ゲートウェイ、接続プロトコル（IPSec または SSL）、オンデマンド ポリシーなどの VPN ポリシー情報が含まれています。

次のいずれかの方法で、Cisco Jabber for iPhone and iPad のアプリケーション プロファイルをプロビジョニングすることができます。

ASDM

ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect セキュア モビリティ クライアントの VPN プロファイルを定義することをお勧めします。

この方法を使用すると、Cisco AnyConnect セキュア モビリティ クライアントが初めて VPN 接続を確立した以降は、VPN プロファイルが自動的にそのクライアントにダウンロードされます。この方法は、すべてのデバイスおよび OS タイプに使用でき、VPN プロファイルを ASA で集中管理できます。

詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Creating and Editing an AnyConnect Profile*」のトピックを参照してください。

iPCU

iPhone Configuration Utility（iPCU）を使用して作成する Apple コンフィギュレーション プロファイルを使用して iOS デバイスをプロビジョニングできます。Apple コンフィギュレーション プロ

ファイルは、デバイスのセキュリティ ポリシー、VPN コンフィギュレーション情報、および Wi-Fi、メール、カレンダーの各種設定などの情報が含まれた XML ファイルです。

高レベルな手順は次のとおりです。

1. iPCU を使用して、Apple コンフィギュレーション プロファイルを作成します。

   詳細については、iPCU の資料を参照してください。

2. XML プロファイルを .mobileconfig ファイルとしてエクスポートします。

3. .mobileconfig ファイルをユーザにメールで送信します。

   ユーザがこのファイルを開くと AnyConnect VPN プロファイルと他のプロファイル設定がクライアント アプリケーションにインストールされます。

MDM

サードパーティの Mobile Device Management（MDM）ソフトウェアを使用して作成する Apple コンフィギュレーションプロファイルを使用して iOS デバイスをプロビジョニングできます。Apple コンフィギュレーションプロファイルは、デバイスのセキュリティポリシー、VPN コンフィギュレーション情報、および Wi-Fi、メール、カレンダーの各種設定などの情報が含まれた XML ファイルです。

高レベルな手順は次のとおりです。

1. Apple 設定プロファイルを作成するには MDM を使用します。

   MDM の使用についての詳細は Apple の資料を参照してください。

2. 登録済みデバイスに Apple 設定プロファイルをプッシュします。

Cisco Jabber for Android のアプリケーション プロファイルをプロビジョニングするには、ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect セキュア モビリティ クライアントの VPN プロファイルを定義します。Cisco AnyConnect セキュア モビリティ クライアントが初めて VPN 接続を確立した以降は、VPN プロファイルが自動的にそのクライアントにダウンロードされます。この方法は、すべてのデバイスおよびOS タイプに使用でき、VPN プロファイルを ASA で集中管理できます。詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Creating and Editing an AnyConnect Profile*」のトピックを参照してください。

VPN 接続の自動化

ユーザが企業の Wi-Fi ネットワーク外から Cisco Jabber を開く場合、Cisco Jabber には、Cisco UC アプリケーション サーバにアクセスするための VPN 接続が必要です。Cisco AnyConnect Secure Mobility Client がバックグラウンドで VPN 接続を自動的に確立できるようにシステムを設定できます。これは、シームレスなユーザ エクスペリエンスの提供に役立ちます。

（注） VPN が自動接続に設定されていても、Expressway for Mobile and Remote Access の方が接続優先順位が高いため、VPN は起動されません。

信頼ネットワーク接続のセットアップ

Trusted Network Detection 機能は、ユーザの場所を基にして VPN 接続を自動化することによって、ユーザの体感品質を向上させます。ユーザが社内 Wi-Fi ネットワークの中にいる場合、Cisco Jabber は直接 Cisco UC インフラストラクチャに到達できます。ユーザが社内 Wi-Fi ネットワークを離れると、Cisco Jabber は信頼ネットワークの外側にいることを自動的に検出します。この状況が発生すると、Cisco AnyConnect セキュア モビリティ クライアントは UC インフラストラクチャへの接続を確保するため VPN を開始します。

（注） Trusted Network Detection 機能には、証明書ベース認証およびパスワード ベース認証の両方を使用できます。ただし、証明書ベース認証の方が、よりシームレスな体感を与えることができます。

手順

ステップ 1 ASDM を使用して、Cisco AnyConnect のクライアント プロファイルを開きます。

ステップ 2 クライアントが社内 Wi-Fi ネットワークの中にいるときにインターフェイスで受信可能な、信頼できる DNS サーバおよび信頼できる DNS ドメイン サフィックスのリストを入力します。Cisco AnyConnect クライアントは、現在のインターフェイス DNS サーバおよびドメイン サフィックスを、このプロファイルの設定と比較します。

（注） Trusted Network Detection 機能が正しく動作するためには、DNS サーバをすべて指定する必要があります。TrustedDNSDomains と TrustedDNSServers の両方をセットアップした場合は、信頼ネットワークとして定義した両方の設定とセッションが一致する必要があります。

Trusted Network Detection をセットアップするための詳細な手順については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Configuring AnyConnect Features*」の章（リリース 2.5）または「*Configuring VPN Access*」の章（リリース 3.0 または 3.1）の「*Trusted Network Detection*」のセクションを参照してください。

Connect On Demand VPN の設定

Apple iOS Connect On Demand 機能は、ユーザのドメインに基づいて VPN 接続を自動化することにより、ユーザ エクスペリエンスを強化します。

ユーザが社内 Wi-Fi ネットワークの中にいる場合、Cisco Jabber は直接 Cisco UC インフラストラクチャに到達できます。ユーザが企業の Wi-Fi ネットワーク外に出ると、Cisco AnyConnect は、AnyConnect クライアント プロファイルで指定されたドメインに接続されているか自動的に検出します。その場合、アプリケーションは VPN を開始して、UC インフラストラクチャへの接続を確認します。Cisco Jabber を含めて、デバイス上のすべてのアプリケーションがこの機能を利用できます。

（注） Connect On Demand は、証明書で認証された接続だけをサポートします。

この機能では、次のオプションを使用できます。

- [常に接続（Always Connect）]：Apple iOS は、常にこのリスト内のドメインへの VPN 接続を開始しようとします。
- [必要に応じて接続（Connect If Needed）]：Apple iOS は、DNS を使用してアドレスを解決できない場合のみ、このリスト内のドメインへの VPN 接続を開始しようとします。
- [接続しない（Never Connect）]：Apple iOS は、このリスト内のドメインへの VPN 接続を開始しようとしません。

注目 Apple は近い将来に、[常に接続する（Always Connect）] オプションを削除する予定です。[常に接続する（Always Connect）] オプションの削除後は、ユーザは [必要に応じて接続する（Connect if Needed）] オプションを選択できます。Cisco Jabber ユーザが [必要に応じて接続（Connect if Needed）] オプションを使用したときに問題が発生する場合があります。たとえば、Cisco Unified Communications Manager のホスト名が社内ネットワークの外部で解決可能な場合は、iOS が VPN 接続をトリガーしません。ユーザは、コールを発信する前に、手動で Cisco AnyConnect セキュア モビリティ クライアントを起動することによって、この問題を回避できます。

手順

ステップ 1 ASDM プロファイル エディタ、iPCU、または MDM ソフトウェアを使用して、AnyConnect クライアント プロファイルを開きます。

ステップ 2 AnyConnect クライアント プロファイルの [必要に応じて接続する（Connect if Needed）] セクションで、オンデマンド ドメインのリストを入力します。
ドメイン リストは、ワイルドカード オプション（たとえば、cucm.cisco.com、cisco.com、および *.webex.com）を含むことができます。

Cisco Unified Communications Manager での自動 VPN アクセスのセットアップ

はじめる前に

- モバイル デバイスで、証明書ベースの認証での VPN へのオンデマンド アクセスが設定されている必要があります。VPN アクセスの設定については、VPN クライアントおよびヘッドエンドのプロバイダーにお問い合わせください。
- Cisco AnyConnect セキュア モビリティ クライアントと Cisco Adaptive Security Appliance の要件については、「ソフトウェア要件」のトピックを参照してください。
- Cisco AnyConnect のセットアップ方法については、『*Cisco AnyConnect VPN Client Maintain and Operate Guides*』を参照してください。

手順

ステップ 1 クライアントがオンデマンドで VPN を起動する URL を指定します。

a) 次のいずれかの方法を使用し、クライアントがオンデマンドで VPN を起動する URL を指定します。

- 必要に応じて接続する（Connect if Needed）
  - Cisco Unified Communications Manager をドメイン名（IP アドレスではなく）経由でアクセスするように設定し、このドメイン名がファイアウォールの外側で解決できないことを確認します。
  - Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを「必要に応じて接続（Connect If Needed）」リストに追加します。
- 常に接続する（Always Connect）
  - 存在しないドメインにステップ 4 のパラメータを設定します。存在しないドメインはユーザがファイアウォールの内部または外部にいるときに、DNS クエリーが失敗する原因となります。
  - Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを「常に接続（Always Connect）」リストに追加します。

    URL は、ドメイン名だけを含む必要があります。プロトコルまたはパスは含めないでください（たとえば、「https://cm8ondemand.company.com/vpn」の代わりに「cm8ondemand.company.com」を使用します）。

b) Cisco AnyConnect で URL を入力し、このドメインに対する DNS クエリーが失敗することを確認します。

ステップ 2 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 3 ユーザのデバイス ページに移動します。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [オンデマンドVPNのURL（On-Demand VPN URL）] フィールドに、ステップ 1 で Cisco AnyConnect で特定して使用した URL を入力します。
URL は、ドメイン名だけを含む必要があります。プロトコルやパスを含まないようにしてください。

ステップ 5 [保存（Save）] を選択します。
Cisco Jabber が開くと、URL への DNS クエリを開始します（たとえば、ccm-sjc-111.cisco.com）。このURLが、この手順で定義したOn Demandのドメイン リストのエントリ（たとえば、cisco.com）に一致する場合、Cisco Jabber は間接的に AnyConnect VPN 接続を開始します。

次の作業

- この機能をテストしてください。
  - この URL を iOS デバイスのインターネット ブラウザに入力し、VPN が自動的に起動することを確認します。ステータス バーに、VPN アイコンが表示されます。
  - VPNを使用して、iOSデバイスが社内ネットワークに接続できることを確認します。たとえば、社内イントラネットのWebページにアクセスしてください。iOSデバイスが接続できない場合は、ご利用の VPN 製品のプロバイダーに問い合わせてください。
  - VPNが特定のタイプのトラフィックへのアクセスを制限（管理者が電子メールと予定表のトラフィックだけが許可されるようにシステムを設定している場合など）していないことを IT 部門に確認します。
- クライアントが、社内ネットワークに直接接続されるように設定されていることを確認します。

AnyConnect マニュアル リファレンス

AnyConnect の要件と展開の詳細については、ご使用のリリースのマニュアルを参照してください。 http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

セッション パラメータ

セキュア接続のパフォーマンスを向上するために ASA セッション パラメータを設定できます。最良のユーザ エクスペリエンスを得るために、次の ASA セッション パラメータを設定する必要があります。

- [Datagram Transport Layer Security]（DTLS）：DTLS は、遅延とデータ消失を防ぐデータ パスを提供する SSL プロトコルです。
- [自動再接続（Auto Reconnect）]：自動再接続またはセッション永続性を使用すれば、Cisco AnyConnect Secure Mobility Client はセッション中断から回復して、セッションを再確立できます。
- [セッション永続性（Session Persistence）]：このパラメータを使用すると、VPN セッションをサービス中断から回復し、接続を再確立できます。
- [アイドルタイムアウト（Idle Timeout）]：アイドル タイムアウトは、通信アクティビティが発生しない場合に、ASA がセキュア接続を切断するまでの期間を定義します。
- [デッドピア検出（Dead Peer Detection）]（DTD）：DTD は、ASA と Cisco AnyConnect Secure Mobility Client が、障害が発生した接続をすばやく検出できることを保証します。

ASA セッション パラメータの設定

Cisco AnyConnect Secure Mobility Client のエンドユーザのユーザ エクスペリエンスを最適化するために、次のように ASA セッション パラメータを設定することを推奨します。

手順

ステップ 1 DTLS を使用するように、Cisco AnyConnect を設定します。
詳細については、『*Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*』の「*Configuring AnyConnect Features Using ASDM*」の章の、「*Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections*」のトピックを参照してください。

ステップ 2 セッションの永続性（自動再接続）を設定します。

a) ASDM を使用して VPN クライアント プロファイルを開きます。

b) [自動再接続の動作（Auto Reconnect Behavior）]パラメータを [復帰後に再接続（Reconnect After Resume）] に設定します。

詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Configuring AnyConnect Features*」の章（リリース 2.5）または「*Configuring VPN Access*」の章（リリース 3.0 または 3.1）の「*Configuring Auto Reconnect*」のトピックを参照してください。

ステップ 3 アイドル タイムアウト値を設定します。

a) Cisco Jabber クライアントに固有のグループ ポリシーを作成します。

b) アイドル タイムアウト値を 30 分に設定します。

詳細については、ご使用のリリースの『*Cisco ASA 5580 Adaptive Security Appliance Command Reference*』の「*vpn-idle-timeout*」のセクションを参照してください。

ステップ 4 Dead Peer Detection（DPD）を設定します。

a) サーバ側の DPD を無効にします。

b) クライアント側の DPD を有効にします。

詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*』の「*Configuring VPN*」の章の、「*Enabling and Adjusting Dead Peer Detection*」のトピックを参照してください。