この統合のための準備

サポートされているドメイン間フェデレーションの統合

このマニュアルでは、IM and Presence サーバと外部ドメインとの間にフェデレーテッド ネットワークを構成するための設定手順について説明します。

IM and Presence サーバがフェデレーションを行える外部ドメインは次のとおりです。

- Microsoft Office Communications Server Release 2007、R2、Microsoft Lync 2010（SIP 経由）

（注） IM and Presence Release 9.0 では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。 OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

- AOL over SIP
- Cisco Webex Connect Release 6.x（XMPP 経由）
- IBM Sametime Server Release 8.2、8.5（XMPP 経由）
- GoogleTalk（XMPP 経由）
- IM and Presence Release 9.0（XMPP 経由）

（注） それぞれ IM and Presence が配置されている 2 つの企業間にフェデレーションを設定する場合は、XMPP フェデレーションの設定方法について記載されている手順に従ってください。

関連トピック

ハードウェア要件, （2 ページ）
ソフトウェア要件, （3 ページ）

ハードウェア要件

Cisco ハードウェア

- IM and Presence サーバ。 IM and Presence のハードウェア サポートについては、IM and Presence の互換性マトリクスを参照してください
- Cisco Unified Communications Manager サーバ。 Cisco Unified Communications Manager のハードウェア サポートについては、Cisco Unified Communications Manager の互換性マトリクスを参照してください
- IM and Presence の企業内に 2 つの DNS サーバ
- Cisco Adaptive Security Appliance（ASA）5500 シリーズ
- （任意）Cisco CSS11506 Content Services Switch
- SIP フェデレーションの場合のみ、TLS プロキシ機能を実現できる Cisco Adaptive Security Appliance（ASA）の使用を推奨します。 XMPP フェデレーションの場合は、いずれのファイアウォールでも十分です。
- **Cisco Adaptive Security Appliance（ASA）**モデルを選択する場合は、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_models_home.html にアクセスしてください。 TLS プロキシ コンポーネントは、すべての 5500 モデルで使用可能です。
- 必ず目的の配置に適したバージョンの Cisco Adaptive Security Appliance（ASA）ソフトウェアを使用してください。 ドメイン間フェデレーションを新たに設定する場合は、IM and Presence の互換性マトリクスで、Cisco Adaptive Security Appliance（ASA）ソフトウェアの適切なバージョンを確認してください。

関連トピック

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html
ソフトウェア要件, （3 ページ）

ソフトウェア要件

Cisco ソフトウェア

- IM and Presence Server Release 9.0
- Cisco Unified Communications Manager Server Release 9.0
- Cisco Adaptive Security Appliance（ASA）v8.3(1)
- Cisco Adaptive Security Device Manager（ASDM）v6.3
- サポートされている XMPP クライアント
  - Cisco Unified Personal Communicator Release 8.5
  - Cisco Jabber for Mac
  - Cisco Jabber for Windows
  - モバイル向け Cisco Jabber IM（Cisco Jabber IM for iPhone、Android、Blackberry）
  - Cisco Jabber for iPad
  - Cisco Jabber for Cius

Microsoft の SIP フェデレーション用ソフトウェア

- Microsoft Lync 2010
- Microsoft OCS 2007 Release 2 Server Standard または Enterprise
- Microsoft Office Communicator 2007 Release 2
- Microsoft Active Directory

AOL の SIP フェデレーション用ソフトウェア

- AOL SIP Access Gateway（SAG）
- AOL Instant Messenger Release 7.2.6.1 以降

XMPP フェデレーション用ソフトウェア

- Cisco Webex Connect Release 6.x
- IBM Sametime Server Release 8.2
- GoogleTalk

関連項目

ハードウェア要件，（2 ページ）

統合の準備

この統合については、綿密な計画を立てることが重要です。 この統合に関する設定を開始する前に、以下の各項目をお読みください。

ルーティング設定

フェデレーテッドネットワークでのルーティングをどのように設定するかを考えます。まず外部ドメイン宛てのメッセージを、IM and Presence から Cisco Adaptive Security Appliance（ASA）を経由して外部ドメインにルーティングする方法について考える必要があります。 その 1 つの選択肢として、IM and Presence の企業配置と Cisco Adaptive Security Appliance（ASA）との間に、ルーティング エンティティ（ルータ、スイッチ、またはゲートウェイ）を配置するという方法があります。 この場合、メッセージはルーティング エンティティから Cisco Adaptive Security Appliance（ASA）にルーティングされ、さらに Cisco Adaptive Security Appliance（ASA）から外部ドメインにルーティングされます。

一方、IM and Presence と外部ドメインとの間に Cisco Adaptive Security Appliance（ASA）をゲートウェイとして配置することもできます。 ローカルな企業配置内で Cisco Adaptive Security Appliance（ASA）を IM and Presence のゲートウェイとして使用する場合は、Cisco Unified Communications Manager および IM and Presence クライアントから IM and Presence サーバへのアクセス方法を考える必要があります。 Cisco Unified Communications Manager および IM and Presence クライアントは、IM and Presence と異なるサブネットに属している場合には、Cisco Adaptive Security Appliance（ASA）を使用して IM and Presence にアクセスする必要があります。

ネットワーク内の既存のファイアウォールの背後に Cisco Adaptive Security Appliance（ASA）を配置する場合は、Cisco Adaptive Security Appliance（ASA）および IM and Presence にトラフィックをルーティングする方法について考える必要があります。 既存のファイアウォール上では、IM and Presence のパブリック アドレスにトラフィックをルーティングするためのルートとアクセス リストを設定します。 また、既存のファイアウォールを使用して、外部ドメインへのルートも設定する必要があります。

関連トピック

Cisco Adaptive Security Appliance（ASA）の配置オプション

SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定

パブリック IP アドレス

SIP フェデレーションの場合、IM and Presence のパブリック アドレスとして、パブリックにアクセスできる IP アドレスが必要です。 割り当てることができる IP アドレスがない場合は、Cisco Adaptive Security Appliance（ASA）の outside インターフェイスを IM and Presenceのパブリック アドレスとして使用してください（Cisco Adaptive Security Appliance（ASA）を在席情報および IM のトラフィック用としてのみ使用している場合）。

Microsoft OCS R2 との SIP フェデレーションでは、複数の IM and Presence サーバを配置する場合でも、必要となるパブリック IP アドレスは 1 つだけです。 Cisco Adaptive Security Appliance（ASA）では、ポート アドレス変換（PAT）を使用して、OCS から適切な IM and Presence サーバへ要求がルーティングされます。

XMPP フェデレーションの場合は、XMPP フェデレーションを有効にした IM and Presence サーバごとにパブリック IP アドレスを公開するか、ただ 1 つのパブリック IP アドレスを公開するかを選択することができます。

- 複数のパブリック IP アドレスを公開する場合は、Cisco Adaptive Security Appliance（ASA）上で NAT を使用してパブリック アドレスをプライベート アドレスに変換します。 たとえば、NAT を使用すると、x.x.x.x:5269 および y.y.y.y:5269 というパブリック アドレスをそれぞれ、a.a.a.a:5269 および b.b.b.b:5269 というプライベート アドレスに変換できます。
- ただ 1 つのパブリック IP アドレスを公開する場合は、Cisco Adaptive Security Appliance（ASA）上で PAT を使用して、正しい IM and Presence サーバにマッピングします。 たとえば、使用するパブリック IP アドレスが x.x.x.x で、かつ _xmpp-server の DNS SRV レコードが複数あるとします。 各レコードのポートはそれぞれ異なりますが、レコードはすべて x.x.x.x に解決されます。 そして外部サーバからは、Cisco Adaptive Security Appliance（ASA）を経由して x.x.x.x:5269、x.x.x.x:15269、x.x.x.x.25269 に要求が送信されるとします。 この場合、Cisco Adaptive Security Appliance（ASA）では、それらの IP アドレスを対象に PAT が実行されます。これにより、それぞれのアドレスは、対応する各 IM and Presence サーバの内部 IP アドレスにマッピングされます。

  たとえば、パブリック IP アドレス x.x.x.x:5269 は a.a.a.a:5269 というプライベート IP アドレス、パブリック IP アドレス x.x.x.x:15269 は b.b.b.b.b:5269 というプライベート IP アドレス、パブリック IP アドレス x.x.x.x:25269 は c.c.c.c:5269 というプライベート IP アドレスにそれぞれマッピングされます。 内部的には、すべての IP アドレスが IM and Presence 上の同一ポート（5269）にマッピングされます。

関連トピック

外部および内部インターフェイスの設定
DNS の設定, （7 ページ）

パブリック FQDN

SIP フェデレーションの場合、要求メッセージのルーティングは FQDN に基づいて行われます。そのため、ルーティング用 IM and Presence サーバ（パブリッシャ）の FQDN は、パブリックに解決可能であることが必要です。

AOL SIP Access Gateway

AOL SIP Access Gateway では、企業の SIP/SIMPLE ベースのインスタント メッセージ サーバと、ネットワーク上のインスタント メッセージ ユーザとの通信を可能にするフェデレーション サービスが提供されます。 AOL SIP Access Gateway を使用すると、企業の SIP/SIMPLE ベースのインスタント メッセージ サーバを利用するユーザは、AIM サービスや AOL サービスのパブリック ユーザと対話することができるほか、その在席情報を取得することもできます。 また AOL SIP Access Gateway により、AIM システムや AOL システムのユーザはインスタント メッセージを送信したり、社内の SIP/SIMPLE ベース システムのユーザに関する在席情報を表示したりすることもできます。

AOL SIP Access Gateway は、内部 AOL プロトコルの変換を行うフロント エンドとして機能します。 企業のサーバと AOL との間の通信は、すべて SIP を使用して行われます。 内部の AOL システムで必要なプロトコルへの変換処理は、AOL SIP Access Gateway で行われるため、 外部サーバに変換機能を追加する必要はありません。そのため、AOL プロトコルは外部からは認識されません。 企業のサーバは、SIP/SIMPLE を使用して通信している場合でも、AOL SIP Access Gateway を介して AOL に接続することが可能です。

AOL SIP Access Gateway は、TLS over TCP を介した接続のみサポートしています。 AOL SIP Access Gateway サーバは、次のアドレスを持つインスタント メッセージ サーバまたはプロキシの内部で定義する必要があります。

サーバ名：sip.oscar.aol.com

サーバ ポート：5061

サーバ名 sip.oscar.aol.com は、205.188.153.55 および 64.12.162.248 に解決されます。

（注）

- これらの IP アドレスをネットワーク内のいずれかの場所で静的に設定した場合は、これらのアドレスが変更されていないかどうか AOL で定期的に確認することをお勧めします。
- また、AOL SIP Access Gateway の FQDN（sip.oscar.aol.com）についても、場合によっては変更される可能性があるため、ping を実行してその IP アドレスを確認することが推奨されます（ping sip.oscar.aol.com など）。

冗長性/ハイ アベイラビリティ

フェデレーテッドネットワークに冗長性を確保する方法についても考える必要があります。Cisco Adaptive Security Appliance（ASA）では、アクティブ/スタンバイ（A/S）導入モデルにより冗長性がサポートされています。

IM and Presence のフェデレーション機能に対してハイ アベイラビリティを実現する必要がある場合は、指定した（フェデレーション）IM and Presence クラスタの手前にロード バランサを配置することができます。 シスコでは、Cisco CSS 11500 Content Services Switch の使用を推奨しています。

Cisco CSS 11500 Content Services Switch のマニュアルは、http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html から入手できます。

DNS の設定

IM and Presence のローカルな企業配置の場合、IM and Presence では、他のドメインが DNS SRV を介して IM and Presence サーバを検出できるように、IM and Presence ドメインに対して DNS SRV レコードをパブリッシュする必要があります。 DNS SRV レコードは、企業の DMZ 内にある DNS サーバに保管されています。

Microsoft OCS R2 との SIP フェデレーションの場合は、DNS SRV レコード「_sipfederationtls」をパブリッシュする必要があります。 Microsoft 製品の企業配置では、IM and Presence をアクセス エッジ サーバ上で Public IM Provider として設定するため、このレコードが必要となります。 外部の企業配置で IM and Presence から Microsoft ドメインを検出できるようにするためには、その外部ドメインを指す DNS SRV レコードが存在する必要があります。 IM and Presence サーバが DNS SRV を使用して Microsoft ドメインを検出できない場合は、IM and Presence 上で、その外部ドメインのパブリック インターフェイスに向かうスタティック ルートを設定する必要があります。

AOL フェデレーションの場合、AOL では「aol.com」ドメインのパブリック DNS サーバで DNS SRV レコード「_sipfederationtls_tcp.aol.com」がパブリッシュされます。 このレコードは、AOL SIP Access Gateway に対応する「sip.oscar.aol.com」に解決されます。

DNS SRV レコードはパブリックに解決可能です。そのため、ローカルの企業配置内で DNS 転送を有効にしている場合は、DNS クエリーを実行することで、外部のパブリック ドメインに関する情報を取得することができます。 DNS クエリーがローカルの企業配置内の DNS 情報に全面的に依存している（ローカルの企業配置内で DNS 転送を有効にしていない）場合は、外部ドメインを指定する DNS SRV レコード/FQDN/IP アドレスをパブリッシュする必要があります。 ただし、その代替手段として、 スタティック ルートを設定することもできます。

XMPP フェデレーションの場合は、DNS SRV レコード「_xmpp-server」をパブリッシュする必要があります。 このレコードにより、フェデレーション XMPP ドメインから IM and Presence ドメインを検出することができるため、両ドメインのユーザは XMPP を介して IM や在席情報をやり取りすることが可能です。 同様に外部ドメインでは、IM and Presence から検出できるよう、パブリック DNS サーバで「_xmpp-server」レコードをパブリッシュする必要があります。

関連トピック

AOL との SIP フェデレーションのルート SIP 要求
AOL との SIP フェデレーションに使用するデフォルト フェデレーション ルーティング ドメインの変更

認証局（CA）サーバ

SIP フェデレーションの場合、IM and Presence の企業配置内の Cisco Adaptive Security Appliance（ASA）と、外部の企業配置とは、セキュアな TLS/SSL 接続を介して IM および在席情報を共有します。

各企業配置では外部 CA により署名された証明書を提示する必要があります。ただし、企業配置ごとに別々の CA が使用される場合もあります。 したがって両者間の相互信頼を実現するためには、それぞれの企業配置に他方の企業配置の外部 CA からルート証明書をダウンロードする必要があります。

XMPP フェデレーションの場合は、セキュアな TLS 接続を設定するかどうかを選択することができます。 TLS を設定する場合は、IM and Presence 上で、外部企業の証明書に署名している認証局（CA）のルート証明書をアップロードする必要があります。 この証明書は、IM and Presence 上の証明書信頼ストア内に存在する必要があります。これは、Cisco Adaptive Security Appliance（ASA）では XMPP フェデレーション用の TLS 接続が終端されないためです。Cisco Adaptive Security Appliance（ASA）は XMPP フェデレーション用のファイアウォールとして機能します。

この統合の前提条件となる設定タスク

- 統合に関する IM and Presence の設定, （8 ページ）
- 統合に関する Cisco Adaptive Security Appliance（ASA）の設定, （9 ページ）

統合に関する IM and Presence の設定

（注） ここで説明する前提条件タスクは、SIP フェデレーションと XMPP フェデレーションのどちらにも共通するものです。

手順

ステップ 1 IM and Presence のインストールおよび設定については、IM and Presence の展開ガイドに記載されている手順に沿って行ってください。
ここでは、IM and Presence が正常に動作することを保証するため、以下のような確認を行います。

- IM and Presence のトラブルシュータを実行します。
- ローカル コンタクトを IM and Presence に追加できるかどうかを確認します。
- クライアントが IM and Presence サーバから在席ステータスを取得できるかどうかを確認します。

ステップ 2 IM and Presence の展開ガイドに記載されている手順に従い、Cisco Unified Communications Manager（CUCM）サーバで、IM and Presence サーバの設定を行います。 IM and Presence サーバの動作に問題がないことを確認します。

関連トピック

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
統合に関する Cisco Adaptive Security Appliance（ASA）の設定, （9 ページ）

統合に関する Cisco Adaptive Security Appliance（ASA）の設定

（注）
- SIP フェデレーションには、Cisco Adaptive Security Appliance（ASA）が必要です。
- XMPP フェデレーションには、ファイアウォールが必要です。 基本的なファイアウォール/NAT/PAT 機能を実現するためであれば、Cisco Adaptive Security Appliance（ASA）を含め任意のファイアウォールを使用することができます。 XMPP フェデレーションで TLS プロキシ機能を実現する場合には、Cisco Adaptive Security Appliance（ASA）は使用しません。

まず、Cisco Adaptive Security Appliance（ASA）をインストールし、その設定を行います。 そのうえで、Cisco Adaptive Security Appliance（ASA）について次のような基本設定の確認を行います。

手順

ステップ 1 コンソールからハイパーターミナル経由で、または Web ベースの Adaptive Security Device Manager（ASDM）から Cisco Adaptive Security Appliance（ASA）にアクセスします。

ステップ 2 Cisco Adaptive Security Appliance（ASA）の適切なライセンスを取得します。 ただし、Cisco Adaptive Security Appliance（ASA）には TLS プロキシのライセンスが必要です。 ライセンス情報については、シスコの担当者にお問い合わせください。

ステップ 3 ソフトウェアをアップグレードします（必要な場合）。

ステップ 4 次のコマンドを使用してホスト名を設定します。

```
(config)# hostname name
```

ステップ 5 [デバイス設定（Device Setup）] > [システム時間（System Time）] > [時計（Clock）] を選択するか、CLI から **clock set** コマンドを使用することにより、ASDM で時間帯、日付、および時刻を設定します。 次の点に注意してください。

- Cisco ASA 5500 の時計は、TLS プロキシを設定する前に設定してください。
- Cisco Adaptive Security Appliance（ASA）では IM and Presence クラスタと同じ NTP サーバを使用することが推奨されます。 Cisco Adaptive Security Appliance（ASA）と IM and Presence サーバとの間で時計が同期されていない場合は、証明書の有効性が確認できないために TLS 接続が正常に確立されないことがあります。
- NTP サーバのアドレスを確認する場合はコマンド ntp server <server_address> を使用してください。また NTP サーバのステータスを確認する場合はコマンド show ntp associat | statusを使用してください。

ステップ 6 Check the Cisco ASA 5500 のモードを確認します。 Cisco ASA 5500 は、デフォルトでシングル モードおよびルーテッド モードが使用されるよう設定されています。

- 現在のモードを確認します。 この値は、デフォルトでシングル モードとなります。

```
(config)# show mode
```

- 現在のファイアウォール モードを確認します。 この値は、デフォルトでルーテッド モードとなります。

```
(config)# show firewall
```

- 外部インターフェイスおよび内部インターフェイスを設定します。
- 基本 IP ルートを設定します。

関連トピック

外部および内部インターフェイスの設定
スタティック IP ルートの設定
統合に関する IM and Presence の設定, （8 ページ）