冗長性確保のためのロード バランサの設定（SIP フェデレーションの場合）

ロード バランサの概要

冗長性とハイ アベイラビリティを持たせるために、フェデレーテッド ネットワークにロード バランサを組み込むことができます。 シスコでは、IM and Presence サーバと Cisco Adaptive Security Appliance（ASA）の間に Cisco CSS 11500 Content Services Switch を配置することを推奨します（SIP フェデレーションのハイ アベイラビリティを参照してください）。

ロードバランサは、Cisco Adaptive Security Appliance（ASA）からの着信 TLS 接続を終端したうえで、TLS 接続を新たに開始して適切なバックエンド IM and Presence サーバへデータをルーティングします。

IM and Presence サーバの更新

冗長性のためにロード バランサを使用する場合は、IM and Presence のパブリッシャ ノードおよびサブスクライバ ノードの設定を更新する必要があります。

手順

タスク	手順
フェデレーション ルーティング パラメータの更新	[サービス（Service）] メニューで [Cisco Unified IM and Presence の管理（Cisco Unified IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] > [Cisco SIP Proxy] の順に選択し、次の値を入力します。 • [バーチャル IP アドレス（Virtual IP Address）]：ロード バランサに設定されているバーチャル IP アドレスを入力します。 1 [サーバ名（Server Name）]：ロード バランサの FQDN に設定します。 2 [フェデレーション ルーティング IM and Presence の FQDN（Federation Routing IM and Presence FQDN）]：ロード バランサの FQDN に設定します。
新規 TLS ピア サブジェクトの作成	1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS ピア サブジェクト（TLS Peer Subjects）] の順に選択します。 2 [新規追加（Add New）] をクリックして、次の値を入力します。 • [ピア サブジェクト名（Peer Subject Name）]：ロード バランサの外部 FQDN を入力します。 • [説明（Description）]：ロード バランサの名前を入力します。
TLS ピア サブジェクト リストへの TLS ピアの追加	1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] の順に選択します。 2 [検索（Find）] をクリックします。 3 [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。 4 ロード バランサ フェデレーション TLS ピア サブジェクトを選択した TLS ピア サブジェクト リストに移動します。

関連トピック

フェデレーション ルーティング パラメータの設定
TLS ピア サブジェクトの新規作成
選択した TLS ピア サブジェクト リストへの TLS ピアの追加

Cisco Adaptive Security Appliance（ASA）の更新

ロードバランサを使用しても、外部ドメインはメッセージをパブリック IM and Presence アドレスに送信しますが、Cisco Adaptive Security Appliance（ASA）によって、このアドレスはロード バランサのバーチャル IP アドレスにマップされます。 つまり、Cisco Adaptive Security Appliance（ASA）は、外部ドメインからメッセージを受信した場合、それをロード バランサに転送するということです。 次に、ロード バランサはそれを該当する IM and Presence サーバに渡します。

このような設定を実現するには、Cisco Adaptive Security Appliance（ASA）を一部変更する必要があります。

- スタティック PAT メッセージの更新, （3 ページ）
- アクセス リストの更新, （6 ページ）
- TLS プロキシ インスタンスの更新, （8 ページ）

スタティック PAT メッセージの更新

ロード バランサの詳細を含むよう、スタティック PAT メッセージを更新する必要があります。

手順

タスク	Cisco Adaptive Security Appliance（ASA）Release 8.2 のコマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 のコマンド
IM and Presence パブリッシャで必要な変更		

タスク	Cisco Adaptive Security Appliance（ASA）Release 8.2 のコマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 のコマンド
パブリック IM and Presence アドレスに対して未使用の任意のポートを使用するよう、スタティック PAT を変更します。	Change: static (inside,outside) tcp <Public IM and Presence IP address> 5061 <Routing IM and Presence private IP address> 5062 netmask 255.255.255.255 to: static (inside,outside) tcp <Public IM and Presence IP address> 55061 <Routing IM and Presence /Publisher private IP address> 5062 netmask 255.255.255.255	object service obj_tcp_source_eq_5061# service tcp source eq 5061 nat (inside,outside) source static obj_host_<Routing IM and Presence Private IP address> obj_host_<public IM and Presence ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061 から object service obj_tcp_source_eq_55061# service tcp source eq 55061 nat (inside,outside) source static obj_host_<Routing IM and Presence Private IP address> obj_host_<public IM and Presence ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_55061

タスク	Cisco Adaptive Security Appliance（ASA）Release 8.2 のコマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 のコマンド

（どのポートでロード バランサが TLS メッセージをリッスンする場合でも）パブリック IM and Presence アドレスに送信されたメッセージを仮想ポート アドレスに転送できるようにする、新しいスタティック PAT を追加します。	`static (inside,outside) tcp <Public IM and Presence address> 5061 <Load Balancer VIP> 5062 netmask 255.255.255.255.`	`object network obj_host_<Loadbalancer VIP>#host <routing IM and Presence private address>`
		
		`object service obj_tcp_source_eq_5061`
		`# service tcp source eq 5061`
		
		`nat (inside,outside) source static obj_host_<LoadBalancer VIP> obj_host_<public IM and Presence ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061`

IM and Presence サブスクライバで必要な変更		

ロード バランサのバーチャル IP アドレスへの新規アクセス リストを追加します。 IM and Presence がアクセスする必要のある外部ドメインごとに、アクセス リストを追加する必要があります。	`access-list ent_lber_to_foreign_ocs extended permit tcp host <subscriber private ip address> host <foreign domain public IP address> 5061`
	
	`access-list ent_lcs_to_lber_routgcup extended permit tcp host <foreign domain public ip address> host <IM and Presence public ip address> 65061`	

ロード バランサのバーチャル IP アドレスが設定されている場合に IM and Presence サーバへのメッセージを開始できるようにする新規アクセス リストを、外部ドメインに追加します。 IM and Presence にアクセスする必要のある外部ドメインごとに、アクセス リストを追加する必要があります。		

関連トピック

スタティック IP ルートの設定
ポート アドレス変換（PAT）

アクセス リストの更新

ロード バランサをサポートするには、導入シナリオに固有の Cisco Adaptive Security Appliance（ASA）のアクセス リストを更新する必要があります。

（注） IM and Presence のパブリック IP アドレスは、Cisco Adaptive Security Appliance（ASA）で DNS レコードに設定されされた、IM and Presence ドメインのパブリック IP アドレスのことです。このレコードには、Cisco Adaptive Security Appliance（ASA）のパブリック IP を含む、ロード バランサの FQDN が記載されます。

手順

導入シナリオ	タスク	設定例
1 つ以上の外部ドメインとのフェデレーションを行う IM and Presence サーバ	新しいロード バランサのバーチャル IP アドレスへの新規アクセス リストを追加します。IM and Presence がアクセスする必要のある外部ドメインごとに、アクセス リストを追加する必要があります。	パブリッシャ： Cisco Adaptive Security Appliance（ASA）Release 8.2 および 8.3 のコマンド： `access-list ent_lber_to_foreign_ocs extended permit tcp host <Virtual IP address> host <foreign domain public IP address> eq 5061`

	ロード バランサのバーチャル IP アドレスが設定されている場合に IM and Presence サーバへのメッセージを開始できるようにする新規アクセス リストを、外部ドメインに追加します。IM and Presence にアクセスする必要のある外部ドメインごとに、アクセス リストを追加する必要があります。	パブリッシャ：
		Cisco Adaptive Security Appliance（ASA）Release 8.2 のコマンド：
		`access-list ent_lcs_to_lber_routgcup extended permit tcp host <foreign domain public ip address> host <cup public ip address> eq 5062`
		Cisco Adaptive Security Appliance（ASA）Release 8.3 のコマンド：
		`access-listent_foreign_server_to_lb extended permit tcp host <foreign public address> host <Loadbalancer Virtual IP address> eq 5062`

	アクセス リストごとに、新しいアクセス リストを組み込むための新しいクラスを追加します。	`class ent_lber_to_foreign_ocs match access-list ent_lber_to_foreign_ocs`
	クラスごとに、IM and Presence によって開始されたメッセージのエントリを policy-map global_policy に作成します。	`policy-map global_policyclass ent_lber_to_foreign_ocs inspect sip sip_inspect tls-proxy ent_cup_to_foreign`
	クラスごとに、外部ドメインで開始されたメッセージのエントリを policy-map global_policy に作成します。	`policy-map global_policyclass ent_lcs_to_lber_routgcup inspect sip sip_inspect tls-proxy ent_foreign_to_cup`

導入シナリオ	タスク	設定例
外部ドメインが 1 つ以上のクラスタ間 IM and Presence サーバを追加している、IM and Presence と IM and Presence のフェデレーション	外部ドメインの ASA は、ローカル ドメインのパブリッシャおよびサブスクライバのために選択された任意のポートへのアクセスを可能にする必要があります。	`access-list ent_cup_to_foreignPubcupwlber extended permit tcp host <foreign domain private CUP address> host <public CUP address of our local domain> 55061` `access-list ent_cup_to_foreignSubcupwlber extended permit tcp host <foreign domain private CUP address> host <public CUP address of our local domain> 65061`
	アクセス リストごとに、新しいアクセス リストを組み込むための新しいクラスを追加します。	
	クラスごとに、policy-map global_policy にエントリを作成します。	

関連トピック

アクセス リストの設定の要件

TLS プロキシ インスタンスの更新

Cisco Adaptive Security Appliance（ASA）で TLS プロキシ インスタンスを更新します。

手順

タスク	設定例

Update TLS-PROXY	変更内容
	
	`tls-proxy ent_foreign_to_cup server trust-point msoft_publicfqdn`
	` client trust-point cup_proxy`
	`  client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
	`!`
	`tls-proxy ent_cup_to_foreign`
	` server trust-point cup_proxy`
	`  client trust-point msoft_publicfqdn`
	`   client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
	
	を、次のように変更します。
	
	`tls-proxy ent_foreign_to_cup server trust-point msoft_publicfqdn`
	` client trust-point msoft_publicfqdn`
	`  client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
	`!`
	`tls-proxy ent_cup_to_foreign`
	` server trust-point msoft_publicfqdn`
	`  client trust-point msoft_publicfqdn`
	`   client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`

関連トピック

TLS プロキシ インスタンスの設定

CA 署名付きセキュリティ証明書の更新

設定にロード バランサを追加する場合は、次の項で説明する、ロード バランサと Cisco Adaptive Security Appliance（ASA）および IM and Presenceサーバの間の CA 署名付きセキュリティ証明書も作成する必要があります。

- ロード バランサと Cisco Adaptive Security Appliance（ASA）の間のセキュリティ証明書の設定, （10 ページ）
- ロード バランサと IM and Presence サーバの間のセキュリティ証明書の設定, （11 ページ）

ロード バランサと Cisco Adaptive Security Appliance（ASA）の間のセキュリティ証明書の設定

このトピックでは、ロードバランサと Cisco Adaptive Security Appliance（ASA）の間でのセキュリティ証明書を設定するために必要な手順の概要を示します。 詳細については、次の URL にある Cisco CSS 11500 Content Services Switch のマニュアルを参照してください。http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

手順

タスク	手順
Cisco Adaptive Security Appliance（ASA）でロード バランサ用の CA 署名付き証明書を作成します。	crypto ca enroll コマンドを使用して、ロードバランサの FQDN を指定します。
Cisco Adaptive Security Appliance（ASA）からロード バランサに CA 署名付き証明書をインポートします。	copy ssl コマンドを使用します。
ロード バランサで Cisco Adaptive Security Appliance（ASA）用の CA 署名付き証明書を作成します。	手順の概要を次に示します（詳細については、『CSS SSL Configuration Guide』を参照してください）。 **1** グローバル設定モードを開始します（config）。 **2** 交換に使用される RSA キー ペアを作成します（ssl genrsa）。 **3** 作成された RSA キー ペアをファイルに関連付けます（ssl associate）。 **4** 証明書署名要求を作成します（ssl gencsr）。 **5** CA からルート CA 証明書を取得します。 **6** CSR を CA に転送します。 **7** 署名証明書をロードバランサに再インポートします（copy ssl および ssl associate）。
ロード バランサから Cisco Adaptive Security Appliance（ASA）に CA 署名付き証明書をインポートします。	crypto ca trustpoint コマンドを使用します。 証明書がインポートされたことを確認するには、show crypto ca certificate コマンドを使用します。

関連トピック

SCEP による登録を使用した Cisco Adaptive Security Appliance（ASA）での証明書の設定
IM and Presence 証明書の Cisco Adaptive Security Appliance（ASA）へのインポート
Microsoft CA を使用した Cisco Adaptive Security Appliance（ASA）と Microsoft アクセス エッジ（外部インターフェイス）の間でのセキュリティ証明書交換

ロード バランサと IM and Presence サーバの間のセキュリティ証明書の設定

このトピックでは、ロードバランサと IM and Presence ノードの間でのセキュリティ証明書を設定するために必要な手順の概要を示します。

手順

タスク	手順
パブリッシャ ノードとサブスクライバ ノードの両方で CA 署名付き証明書を作成します。	CA署名付き証明書を使用して証明書を交換する手順に従ってください。
（パブリッシャ ノードとサブスクライバノードから）ロードバランサに CA 署名付き証明書をインポートします。	copy sslおよびssl associate コマンドを使用します。

Microsoft コンポーネントの更新

ロードバランサの詳細を使用して、一部の Microsoft コンポーネントを更新する必要があります。

手順

タスク	手順
FQDN のすべてのインスタンスをロードバランサの FQDN に一致するよう更新します。	

タスク	手順
ロード バランサを使用して、IM プロバイダ リストのドメイン名を更新します。	1 外部アクセス エッジ サーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。 2 左側のペインで [Microsoft Office Communications Server 2007] を右クリックします。 3 [IM プロバイダ（IM Provider）] タブをクリックします。 4 [追加（Add）] をクリックします。 5 [この IM サービス プロバイダを許可する（Allow the IM service provider）] をオンにします。 IM サービス プロバイダのネットワーク アドレスをロード バランサのパブリック FQDN として定義します。

関連トピック

SIP フェデレーションに関する外部サーバ コンポーネントの設定

AOL コンポーネントの更新

ご使用の AOL フェデレーション導入にロード バランサを組み込む場合は、ロード バランサに関するいくつかの細目を AOL に提供する必要があります。 詳細については、関連項目内の項を参照してください。

関連トピック

AOL との SIP フェデレーションの要件

ロード バランサ設定

このトピックでは、この統合をサポートするために、Cisco CSS 11500 Content Services Switch を設定する際に必要となるタスクの概要を示します。 Cisco CSS 11500 Content Services Switch をバックエンド SSL モードで使用する場合、SSL アクセラレータ モジュールをインストールおよび設定する必要があります。各タスクの詳細については、次の URL にある Cisco CSS 11500 Content Services Switch のマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

手順

タスク	追加の注意事項
Cisco CSS 11500 Content Services Switch と IM and Presence の間の証明書交換を設定します。	• CA または自己署名証明書は、SSL モジュールで使用できます。 • Cisco CSS 11500 Content Services Switch 用の証明書を作成して、リモート サーバにインポートする必要があります。 • リモート サーバからの証明書を Cisco CSS 11500 Content Services Switch にインポートする必要があります。
Cisco CSS 11500 Content Services Switch と Cisco Adaptive Security Appliance（ASA）の間の証明書交換を設定します。	
SSL モジュールが適切にクライアントからの SSL 通信を処理、終了し、サーバへの HTTP 接続を開始できるよう、SSLプロキシリストに仮想 SSL サーバを定義する必要があります。	• Cisco Adaptive Security Appliance（ASA）がポイントしているIPアドレスおよびポート番号を指定する必要があります。 • Cisco Adaptive Security Appliance（ASA）に対して、既存の証明書の名前とキー ペアを指定する必要があります。
IM and Presence サーバごとに、SSL プロキシ リスト内にバックエンド SSL サーバ エントリを作成します。	• IM and Presence サーバのアドレスを指定する必要があります。 IM and Presence サーバ（バックエンド サーバ）は、VIP のアドレスとは異なるサブネットに含まれている必要があります。 • バックエンド サーバ接続には、フロントエンドと異なる TLS 暗号スイートか TCP を使用できます。 • Cisco CSS 11500 Content Services Switch で TLSのトラフィックを受信するポートを指定する必要があります。 • TLS のトラフィックを IM and Presence サーバに送信するポートを指定する必要があります。

タスク	追加の注意事項
IM and Presence サーバごとに、SSL 終了用の SSL サービスを作成します。	• キープアライブ ポートを指定する場合、ポート番号は、バックエンド SSL サーバ エントリ用に設定したのと同じポート番号にする必要があります。 • キープアライブ メッセージ タイプの値は「tcp」である必要があります。
SSL モジュールを作成します。	• SSL モジュールの物理スロット番号を指定する必要があります。 CSS コマンド "show chassis" を使用して、このスロット番号を取得します。 • SSL モジュールでは、IM and Presence サーバを SSL サービスに関連付ける必要があります。たとえば、**ssl_list1** という SSL プロキシ リストを追加します。
復号化されたデータを ASA から IM and Presence サーバにルーティングする内部コンテンツ ルールを作成します。	
復号化とロードバランシングのために TLS データを SSL モジュールにルーティングするコンテンツ ルールを作成します。	
VIP と IM and Presence バックエンド サーバの間の NAT 割り当てを作成します。	
IM and Presence と Microsoft OCS の間で直接（Cisco Adaptive Security Appliance（ASA）なしで）Cisco CSS 11500 Content Services Switch を使用する場合は、OCS を使用して、IM and Presence サーバの証明書件名共通名を IM and Presence の IP アドレスに解決できることが必要です。 また、すべての IM and Presence サーバの件名共通名が OCS ホスト承認リストに記載されている必要があります。	