構築ガイド

Microsoft Lync Server 2013
AX/Thunder 構築ガイド

Document No. : DG_AXTHLync_20131219 Ver.1.2

Date : 2014/6/02

目次

1 はじめに

AX/Thunder シリーズアプリケーションサービスゲートウェイは、Microsoft Lync 2013 の新機能やアプリケーションに対応した高度なロードバランシングサービスを提供します。Lync の展開に関連してハードウェアとソフトウェア(SoftAX)の両バージョンが、マイクロソフト社により認定されています。

A10 ネットワークスはマイクロソフト社とのパートナーシップを通じ、マイクロソフト社の認定を取得しマイクロソフト社製品向けの各種展開ガイドを提供しています。A10 ネットワークスは、Office Communication Server （OCS）2007 R2 並びに Lync Server 2010 同様、マイクロソフト社のユニファイドコミュニケーション製品を今後も継続してサポートしていきます。

Microsoft Lync Server 2013 では、数多くの新機能がリリースしされましたが、過去オプション機能として存在していた、アーカイブ・モニタリング機能、A/V 会議機能(大規模展開時に必要) がフロントエンドサーバーに統合されたことを除き、ネットワークトポロジに大きな変更はありません。また、Lync Server 2010 で展開を推奨されていたディレクター役割は、Lync Server 2013 ではオプション扱いとなっています。フロントエンドサーバーがディレクター役割を代行することで、全体のサーバー台数を削減することができるアーキテクチャとなっています。

マイクロソフト社は、Lync のリバースプロキシとして推奨していた [1] Threat Management Gateway (TMG) 2010 の販売を終了しました。A10 ネットワークスの AX/Thunder シリーズ製品は、TMG 2010 同様、外部ネットワーク上のデバイス(Lync モバイル、Lync Web Apps 等)から内部の Lync システムへのセキュアな通信を実現する Lync のリバースプロキシとして動作します。AX/Thunder は、TMG 2010 が持ち合わせているセキュリティ機能を補完し、TMG からのシームレスな移行をサポートします。また、AX/Thunder のセキュリティ機能は今後更なる拡張を予定しております。

[1] http://technet.microsoft.com/ja-jp/forefront/bb852242

1.1 構築ガイドの概要

本書では、A10 ネットワークの AX/Thunder シリーズアプリケーションサービスゲートウェイおよび Lync のサーバーロードバランサ構成手順に従い、Microsoft Lync 2013 エンタープライズサーバーエディションをサポートする構成について順を追って説明していきます。本書の内容は、Microsoft Lync 2013 エンタープライズサーバーエディションでテストして確認しております。Microsoft OCS 2007 の構築にあたり本書を使用することはできません。Microsoft OCS 向け AX/Thunder 構築ガイドについては、別途 www.a10networks.com を参照してください。

下記のラボトポロジ(図 1)は、内部および外部のユーザに対し高可用性を備えた Lync 音声、IM/プレゼンス、デスクトップ共有および会議コミュニケーションをサポートできるようにすることを目的として設計されています。このラボトポロジは、フロントエンドプールに 3 台のサーバーを使用して構築されていますが、必要に応じてサーバーを追加することができます。

このラボトポロジは、Lync 展開で必要な 4 つのネットワークをサポートするにあたり 1 組の A10 Networks ロードバランサを使用して構築されています。4 つのネットワークは、内部(フロントエンド)、内部エッジ、外部エッジ並びにリバースプロキシです。

ラボトポロジ

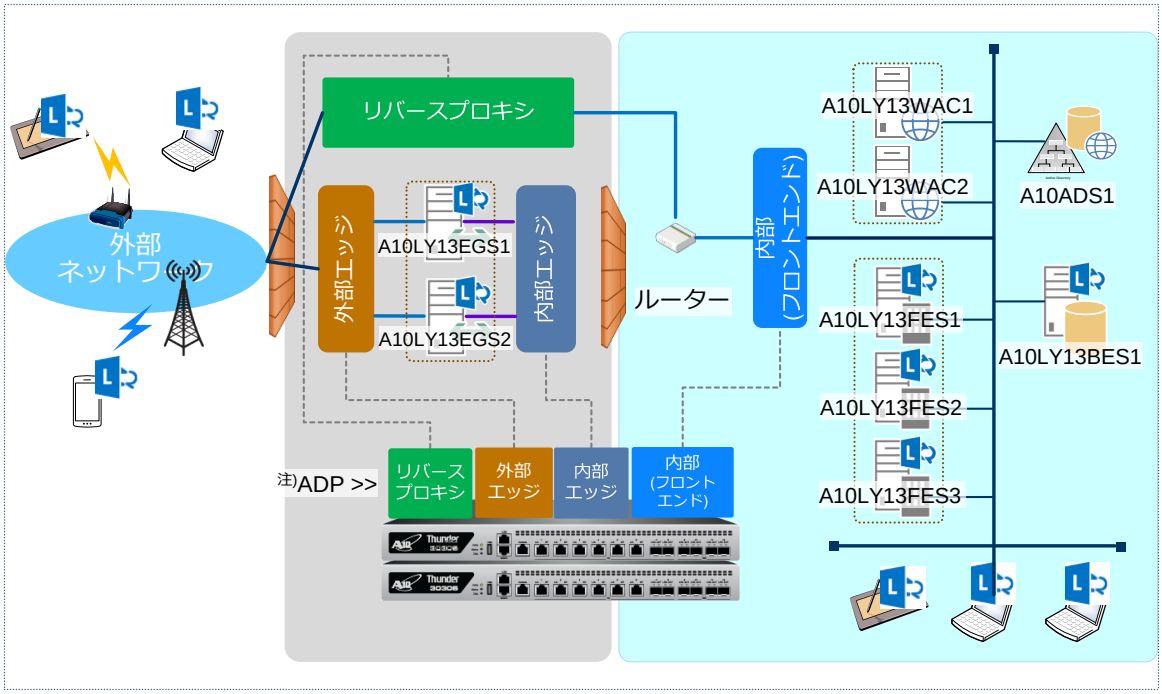

図 1：ラボトポロジ

注) ADP : Application Delivery Partitions とは、1 台の AX/Thunder 上に複数パーティションを構成できる機能となります。

役割	VIP	ホスト名	IP アドレス
AD/内部 CA/内部 DNS	–	A10ADS1	192.168.10.14/24
フロントエンド	192.168.10.82/24	A10LY13FES1	192.168.10.17/24
		A10LY13FES2	192.168.10.18/24
		A10LY13FES3	192.168.10.19/24
バックエンド	–	A10LY13BES1	192.168.10.20/24
エッジ外部	172.17.0.111, 112, 113/24	A10LY13EGS1	172.17.0.21, 22, 23/24
		A10LY13EGS2	172.17.0.31, 32, 33/24
エッジ内部	172.19.0.101/24	A10LY13EGS1	172.19.0.121/24
		A10LY13EGS2	172.19.0.131/24
Office Web Apps	192.168.10.86/24	A10LY13WAC1	192.168.10.23/24
		A10LY13WAC2	192.168.10.24/24

注：CA：Certificate Authority の略で、認証局となります。

1.2　本書の前提条件

本書の内容は、以下の前提条件に基づいてテストされています。

- AX/Thunder の ACOS バージョンは 2.7.1-p2 で、Lync の各役割向け負荷分散等を実現するにあたり ADP を利用しています。
- Lync Server 2013 の音声、インスタントメッセージ(IM)、プレゼンス、デスクトップコラボレーション、および音声ビデオ(AV)の会議アプリケーションについてテストで動作確認を実施しました。テストは、内部ユーザと外部ユーザの両方で実施しています。
- テストは、Microsoft Lync 2013 エンタープライズサーバーエディションと共に Microsoft SQL Server 2012 エンタープライズエディションバージョン 11.00.2100.60 を使用しています。
- Lync Server 2013 のすべてのコンポーネント(Office Web Apps サーバー含)は Windows Server 2012 (64 ビット) Standard Edition オペレーティングシステム上に構成されています。
- Lync クライアントとして、Lync 2013(Windows 7 オペレーティングシステム)、iPhone 向け Lync モバイル 5.1 を使用しています。
- AX/Thunder はワンアームで構成されています。

1.3 Lync Server 2013 のサーバー役割

Lync ソリューションには複数のサーバー役割が含まれています。以下にそれらサーバー役割について記します。

フロントエンドサーバー – Lync Server 2013 のフロントエンドサーバーは、Lync Server 2010 と同様の機能を提供します。ユーザ認証・登録、音声、IM/プレゼンス、Web 会議およびアプリケーション共有機能を提供します。また、アドレス帳サービスや配布リストも提供します。フロントエンドサーバーは、フロントエンドプール内にプロビジョニングされ、拡張性および冗長性・復元性を提供するため、すべて同じ構成となります。

Active Directory ドメインサービス(AD DS) - トポロジ内で参照されるすべての Lync Server は Active Directory ドメインサービス(AD DS)に参加する必要があります。ただし、エッジサーバーは例外です。Lync ユーザは、Active Directory ドメインおよび Lync Server 2013 コントロールパネル(CSCP)内で管理されます。Active Directory ドメインサービスは Lync Server 2013 の展開で必須となります。

バックエンドサーバー - フロントエンドプールにデータベースサービスを提供する Microsoft SQL Server です。バックエンドサーバーは、プール内ユーザデータ、会議データ用のバックアップストアとして動作し、応答グループサービス等のその他データベースのプライマリストアとなります。SQL サーバーは、単一のバックエンドサーバーとして構成できますが、冗長性を実現するにあたり、複数のサーバーをクラスタとして構成することが推奨されています。

エッジサーバー - エッジサーバーを展開すると、外部ユーザは内部ユーザまたは外部ユーザとコミュニケーション、コラボレーション作業を行うことができます。冗長性実現のため、複数のエッジサーバーをエッジサーバープールに配置することができます。エッジサーバーはまた Skype、Windows Live、AOL、Yahoo および Google Talk などのサードパーティの IM サービスへの接続にも利用します。

2 AX/Thunder の構成

AX/Thunder は以下の管理インターフェースを提供します。

- コマンドラインインターフェース(CLI) –

  コマンドライン上で直接コマンドを入力するテキストベースのインターフェース。以下のプロトコルのいずれかを使用して、シリアルコンソールまたはネットワーク経由で CLI に直接アクセス可能です。

  - セキュリティで保護されたプロトコル – Secure Shell (SSH)バージョン 1 または 2
  - セキュリティで保護されていないプロトコル – Telnet (利用可能な環境の場合)

- グラフィカルユーザインターフェース(GUI) –

  クリックして構成ページまたは管理ページにアクセスし、値を入力または選択してデバイスの構成または管理を実行する Web ベースのインターフェース。GUI には、セキュリティで保護されたプロトコル – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) を使用します。

  注：AX/Thunder では、http 要求は https にデフォルトでリダイレクトされます。

デフォルトでは、Telnetのアクセスは、管理インターフェースをはじめとするすべてのインターフェースで無効です。また、SSH、HTTPおよびHTTPSはデフォルトで管理インターフェース上のみ有効で、その他すべてのデータインターフェース上ではデフォルトで無効となっています。

2.1 CLI へのログイン

AX/Thunder には、管理アクセスをセキュリティで保護する高度な機能が備わっています。このセクションでは、デフォルトのセキュリティ設定が適用されていることを前提とします。

SSH を使用して CLI にログインするには、以下の手順を実行します。

1. AX/Thunder の管理インターフェースにアクセス可能なネットワークに接続した PC 上で、管理インターフェースの IP アドレスを使って SSH 接続を開きます。

   注：AX/Thunderの管理インターフェースのデフォルトのIPアドレスは、172.31.31.31です。

2. 通常、SSH クライアントが AX/Thunder に初めて接続すると、SSH クライアントから安全上の警告が表示されます。警告を注意深く読み、警告に同意して接続を完了します。(Enter キーを押します)。
3. login as:プロンプトにユーザ名として”admin”を入力します。
4. Password:プロンプトに admin パスワード(初期値は”a10”)を入力します。admin ユーザ名とパスワードが有効な場合は、CLI の User EXEC レベルのコマンドプロンプトが表示されます。

   AX>

   User EXEC レベルでは、show コマンドに加え、ping や traceroute などのいくつかの基本コマンドを利用できます。

注：CLIプロンプトには「AX」もしくは「ACOS」が表示されます。これは、デバイス上に構成されているホスト名を表しております。ホスト名を変更した場合には、設定したホスト名がプロンプトに表示されます。

5. CLI の Privileged EXEC レベルにアクセスし、すべての構成レベルにアクセスできるようにするには、”enable”コマンドを入力します。Password:プロンプトに enable パスワードを入力します(初期ではパスワード無となっております)。このパスワードは admin パスワードとは異なりますが、どちらのパスワードにも同じ値を構成することは可能です。

   enable パスワードが正しい場合は、CLI の Privileged EXEC レベルのコマンドプロンプトが表示されます。

   AX#

6. グローバル構成レベルにアクセスするには、”config”コマンドを入力します。構成モードでは以下のコマンドプロンプトが表示されます。

   AX(config)#

2.2 AX/THUNDER グラフィカルユーザインターフェース(GUI)へのログイン

ブラウザで、https://"管理インターフェースの IP アドレス"を入力すると、以下のログインダイアログが表示されます。

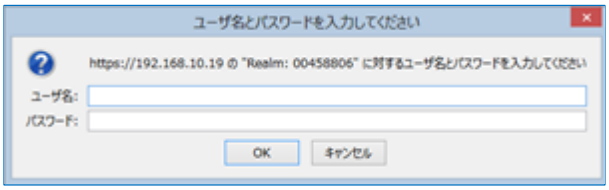

図2：GUIログイン画面

注：ダイアログの名前と外観は、使用しているブラウザに応じて異なります。

注：AX/Thunderが利用しているWebサーバー証明書を発行した認証局(AX/Thunder内部の認証局)のルート証明書が、アクセスしているPC上の信頼されたルート証明機関に存在しないため、最初のアクセス時にはエラーがでますが、セキュリティ例外と処理することにより上記ログイン画面が表示されます。

1. admin **ユーザ名**と**パスワード(デフォルト"a10")**を入力し、[OK]をクリックします。

AX/Thunder の情報がひと目でわかるサマリーページが開きます。GUI 使用中はこのページにいつでもアクセスできます。それには、**[モニタ]** > **[概要]** > **[サマリ]**を選択します。

3 構成要件表

以下の表は、Lync Server 2013 エンタープライズエディションの展開に必要なサービスのリストです。

表 1：Lync フロントエンドサーバー(必須)

サービス名	ポート	VIP タイプ	ソース NAT	機能テンプレート	メモ
Lync フロントエンドサービス	135	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	ユーザの移動、ユーザレプリケータ同期、およびアドレス帳同期などの DCOM ベースの操作で使用。
Lync Server Web 互換性サービス	443	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	フロントエンドサーバーから Web ファーム FQDN (IIS Web コンポーネントで使用される URL)への通信に使用。 SSL オフロードを利用する場合には、クライアント SSL テンプレートが必要。
Web サーバーコンポーネント	4443	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	外部アクセスのための Web コンポーネントで使用。 SSL オフロードを利用する場合には、クライアント SSL テンプレートが必要。
Lync Server Web 互換性サービス	444	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	会議の状態を管理する Lync Server コンポーネントと個別のサーバー間の通信で使用。
Lync フロントエンドサービス	5061	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	サーバー間のすべての内部 SIP 通信 (MTLS)、サーバーとクライアントの間の SIP 通信(TLS)、およびフロントエンドサーバーと仲介サーバーの間の SIP 通信 (MTLS) において、フロントエンドプールで使用

表 2：Lync フロントエンドサーバー (オプション)					
サービス名	ポート	VIP タイプ	ソース NAT	機能テンプレート	メモ
Lync Server アプリケーション共有サービス	5065	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	アプリケーション共有の SIP リッスン要求を受信するためのポート。
Lync Server 応答グループ サービス	5071	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	応答グループアプリケーションの SIP 要求を受信するためのポート。
Lync Server 会議アテンダント サービス (ダイヤルイン会議)	5072	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	Microsoft Lync 2010 Attendant (ダイヤルイン会議)の SIP 要求を受信するためのポート。
Lync Server 会議アナウンス サービス	5073	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	Lync Server 会議アナウンスサービスの SIP 要求を受信するためのポート。
Lync Server コールパーク サービス	5075	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	コールパークアプリケーションの SIP 要求を受信するためのポート。
Lync Server オーディオ テスト サービス	5076	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	オーディオ テスト サービスの SIP 要求を受信するために使用。

注：Lync フロントエンドサーバーのポートとプロトコルに詳細については以下で確認できます。

http://technet.microsoft.com/ja-jp/library/gg398833.aspx

表 3：内部エッジサーバー

サーバーの役割	ポート	VIP タイプ	ソース NAT	フィーチャテンプレート	使用上の注意
内部エッジ サーバー	443	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	内部エッジサーバーとファーム FQDN との間の通信で使用。
内部エッジ サーバー	3478	UDP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	内部ユーザと外部ユーザ間のメディア転送(UDP)の推奨パス。
内部エッジ サーバー	5061	TCP/TLS	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	リモートユーザアクセスまたはフェデレーションの SIP/MTLS 通信用の外部ポートに使用。
内部エッジ サーバー	5062	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	AV エッジのユーザ認証で使用

注：Lync エッジサーバーのポートとプロトコルに詳細については以下で確認できます。

http://technet.microsoft.com/ja-JP/library/gg398739.aspx

表 4：外部エッジサーバー					
サーバーの役割	ポート	VIP タイプ	ソース NAT	機能テンプレート	メモ
外部エッジ アクセス	443	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	すべての内部メディア通信にアクセスする、リモートユーザのアクセス用の SIP/TLS 通信で使用されるポート。
外部エッジ アクセス	5061	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	リモートユーザのアクセスとフェデレーション用の外部 SIP/MTLS 通信に使用されるポート。
外部エッジ WebConf	443	TCP	Auto	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	すべての内部メディア通信にアクセスする、リモートユーザのアクセス用の SIP/TLS 通信で使用されるポート。
外部エッジ AV	443	TCP	-	パーシステンス：SIP (ソース IP) TCP：TCP-Lync ヘルスモニタ：HM	すべての内部メディア通信にアクセスするリモートユーザのアクセス用の SIP/TLS 通信で使用されるポート。
外部エッジ AV	3478	UDP	-	パーシステンス：SIP (ソース IP) ヘルスモニタ：HM	STUN/UDP の受信用および送信用のメディアリソースで使用。

注：外部エッジプールの展開時に、Lync エッジサーバープールを単一の FQDN および IP アドレスまたは複数の FQDN および IP アドレスで展開するかどうかを尋ねる機能選択が表示されます。[単一 FQDN および IP アドレス使用]の機能選択を解除すると、外部エッジプールで複数 IP 構成が可能になります。AX/Thunder は単一 IP 構成と複数 IP 構成のどちらの展開でもサポートしています。複数 IP 構成の場合はアクセス、Web 会議および AV エッジ向けに 3 つのパブリック IP アドレスが必要となります。単一の FQDN および IP アドレス構成では、パブリック IP アドレス(VIP)は 1 つだけ必要となります。

プロトコルの定義

STUN - Session Traversal Utilities for NAT (STUN)
SIP- Session Initiation Protocol (セッション開始プロトコル)
MTLS - Multiplexed Transport Layer Security
PSOM - Persistent Shared Object Protocol
TLS -Transport Layer Security (トランスポート層セキュリティ)
FQDN -Fully Qualified Domain Name (完全修飾ドメイン名)
DCOM - Distributed Component Object Model (分散コンポーネントオブジェクトモデル)

表 5：Office Web Apps サーバー(オプション)					
サービス名	ポート	VIP タイプ	ソース NAT	機能テンプレート	メモ
Office Web Apps サーバーサービス	443	TCP	Auto	パーシステンス：persistence-wac (クッキー) ヘルスモニタ：WAC-80 クライアント SSL テンプレート：wac-hlb-c-ssl	Lync Server 2013 環境で、パワーポイント資料共有を実行する際に、Lync クライアントと Office Web Apps サーバー間の通信で使用。 SSL オフロードを利用する場合には、クライアント SSL テンプレートが必要。

表 6：リバースプロキシ(オプション)					
サービス名	ポート	VIP タイプ	ソース NAT	機能テンプレート	メモ
Lync 外部公開 Web サービス	443 >> 4443	TCP	Auto	パーシステンス：cookie-RP (クッキー) クライアント SSL テンプレート：RP-Client-SSL サーバーSSL テンプレート：RP-Server-SSL aFleX : Lync-WAC-Selection	Lync Server 2013 環境で、外部からの Web サービスへの通信を内部の Lync サーバーへ中継する際に使用。 外部公開ポート番号は 443 で、中継先の Lync サーバーのポート番号は 4443 を使用。
Office Web Apps 外部公開サービス	443	TCP	Auto	上記 Lync 外部公開 Web サービスの設定を利用するため、専用の機能テンプレートは無	Lync Server 2013 環境で、パワーポイント資料共有を実行する際に、Lync クライアントと Office Web Apps サーバー間の通信で使用。

注 :リバースプロキシのポートとプロトコルに詳細については以下で確認できます。

http://technet.microsoft.com/ja-JP/library/jj204932.aspx

3.1　機能テンプレートと構成テンプレート

以下のテンプレートおよび構成は、特定のサーバー役割に必要です。構成要件表を参照してください。

A. TCP タイムアウトテンプレートを作成するには：

1. **[コンフィグ]** > **[サービス]** > **[テンプレート]** > **[L4]**の順に選択します。
2. [追加]をクリックし、以下の設定を実行します。
    a. [名前]：**TCP－Lync**
    b. [アイドルタイムアウト] ：**1200**
    c. [リセット送信(サーバー)] ：**有効**
    d. [リセット送信(クライアント)] ：**有効**
3. 完了したら、**[OK]**をクリックし、**[保存]**をクリックします。

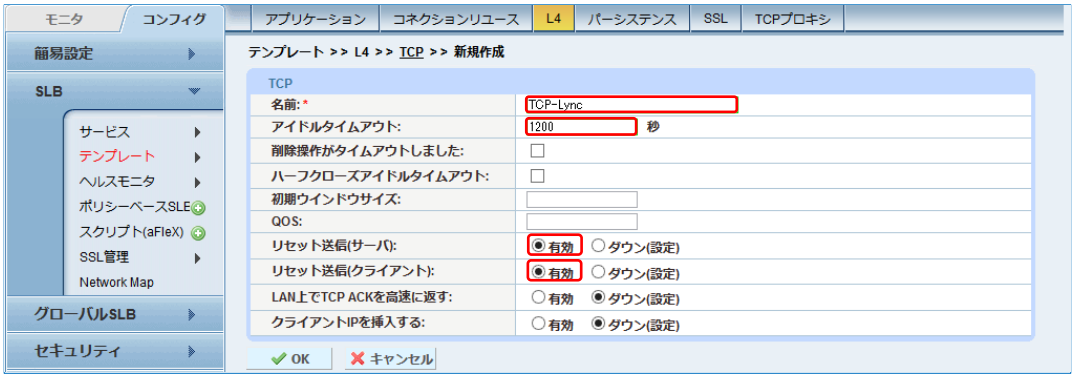

図 3：L4 TCP テンプレート

注：1200秒のTCPアイドルタイムアウトは、AX/ThunderでTCP接続がリセットされるまでに必要なアイドル時間です。

B. ソース IP パーシステンスを作成する方法：

1. **[コンフィグ] > [SLB] > [サービス] > [テンプレート] > [パーシステンス]** の順に選択します。
2. ドロップダウンリストから**[ソース IP パーシステンス]**を選択します。
3. **[追加]**をクリックし、以下の設定を実行します。
   a. [名前]： **SIP**
   b. [マッチタイプ]：**サーバー**
   c. [タイムアウト]：「**20**」分
   d. [ネットマスク]：**255.255.255.255** (デフォルト)
4. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。

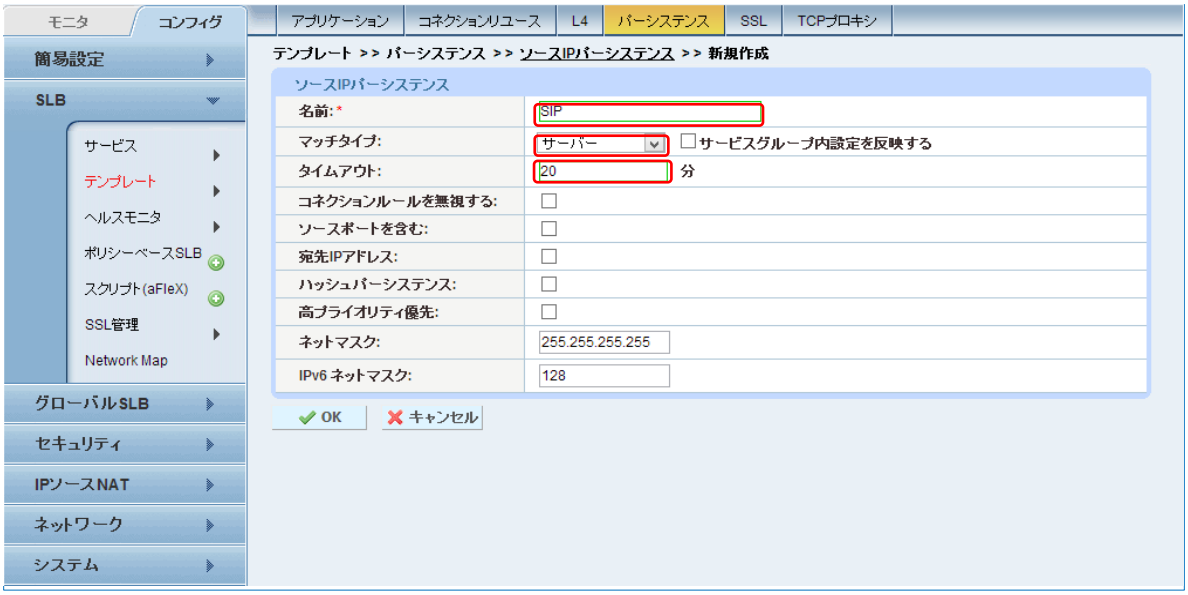

図 4：ソース IP パーシステンステンプレート

C. ヘルスモニタを作成する方法：

1. **[コンフィグ] > [SLB] > [ヘルスモニタ] > [ヘルスモニタ]**の順に選択します。
2. **[追加]**をクリックし、以下の設定を実行します。
   a. [名前]：**HM**
   b. その他はデフォルト値
3. 完了したら、**[OK]**をクリックし、**[保存]**をクリックします。

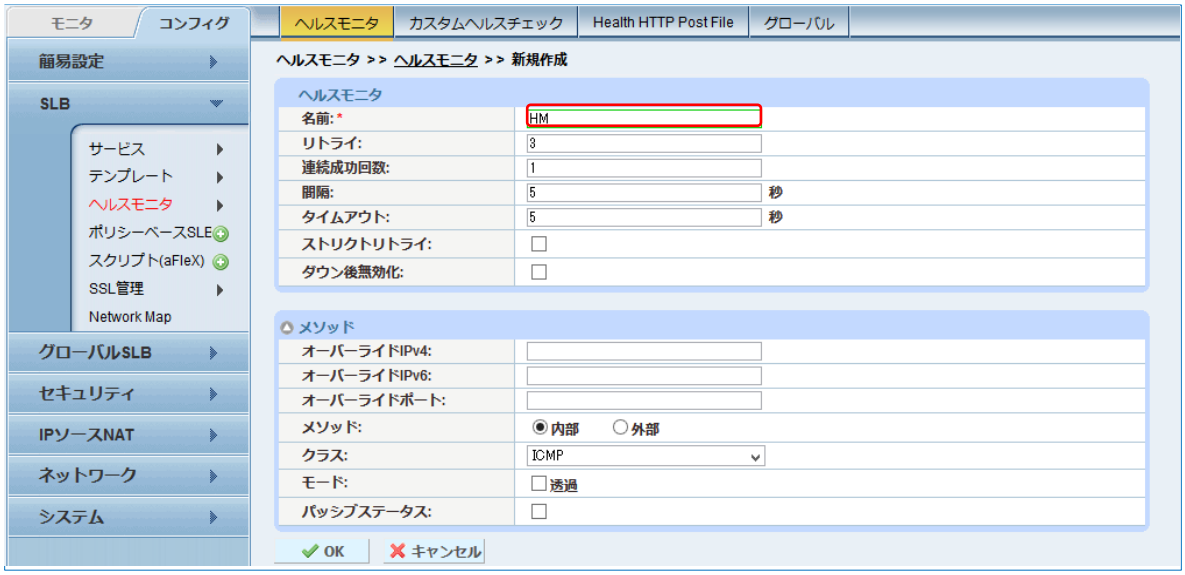

図 5：ヘルスモニタ

4. 続いて同様の手順で、Lync SIP 向けのヘルスモニタを以下の設定内容で構成します。

   a. [名前] : **SIP 5060**

   b. [間隔] : **15 秒**

   c. [タイムアウト] : **5 秒**

   注 : 間隔やタイムアウト値は、既存のネットワーク・サーバー監視ポリシーに準じるべきと考えますので、IT 部門等の管理されているご担当へご相談ください。

   d. [クラス] : **SIP**

   e. [ポート] : **5060**

   f. [TCP] **: チェック**

   g. [レスポンスコード] **: 401,448**

5. 完了したら、**[OK]**をクリックし、**[保存]**をクリックします。

注：上記ヘルスモニタは、サーバーのヘルスモニタで使用してください。監視ポート番号 TCP/5060 は実際の使用ポート TCP/5061 と一致しないため、TCP/5061 を定義しているサービスグループやサーバーポートでは動作しませんので注意願います。

注**:** TCP ポートベースのヘルスチェックも構成することができます。TCP ポートヘルスチェックを利用する場合には、使用する全てのポート分を設定する必要があります。

以下は構成例です。

   a. [名前] : **TCP 443**

   b. [間隔] : **30**

   c. [タイムアウト] : **10**

   d. [クラス] : **TCP**

   e. [ポート] : **443**

   f. [ハーフオープン] **: 無効**

D. フロントエンドサーバーでの SIP モニタの構成方法：

この設定は、Lync Server 2013 トポロジビルダーで Enterprise Edition フロントエンドプールを選択して有効にできます。この機能の目的は、A10 ネットワークス社 AX/Thunder でポート 5060 を利用して Lync サーバーの状態を監視できるようにすることです。

1. Lync フロントエンドサーバーのいずれかから**Lync Serverトポロジビルダー**を起動します。
2. 既存の展開から**[トポロジのダウンロード]**を選択して構成を保存します。
3. **[Enterprise Edition フロントエンドプール]** の名前を選択します。
4. 本構成では、プール名「lync2013.a10domain.a10.local」のプロパティを編集します。[ロード バランサー機器の監視ポートの有効化]チェックボックスをオンにし、「**5060**」と入力して[**OK**]をクリックします。

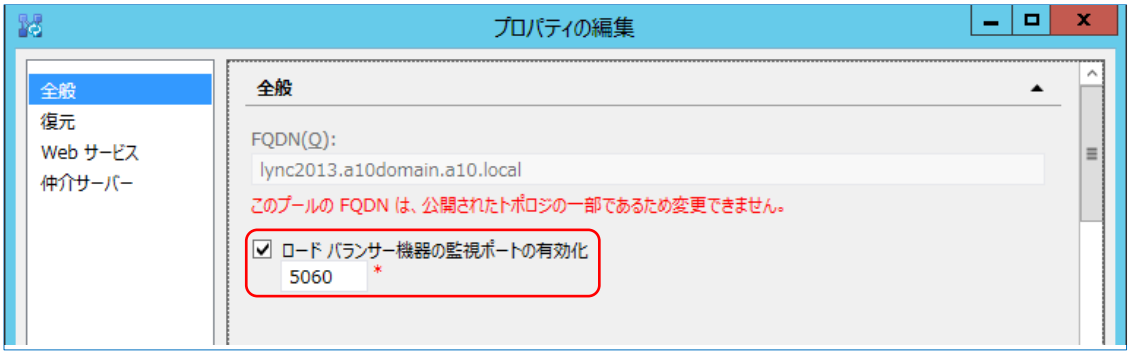

図6：Microsoft Lync での全般プロパティの編集

5. プール名を右クリックし、**[トポロジ]** > **[公開]**を選択し、変更した Lync トポロジを公開して、データベースに反映させます。

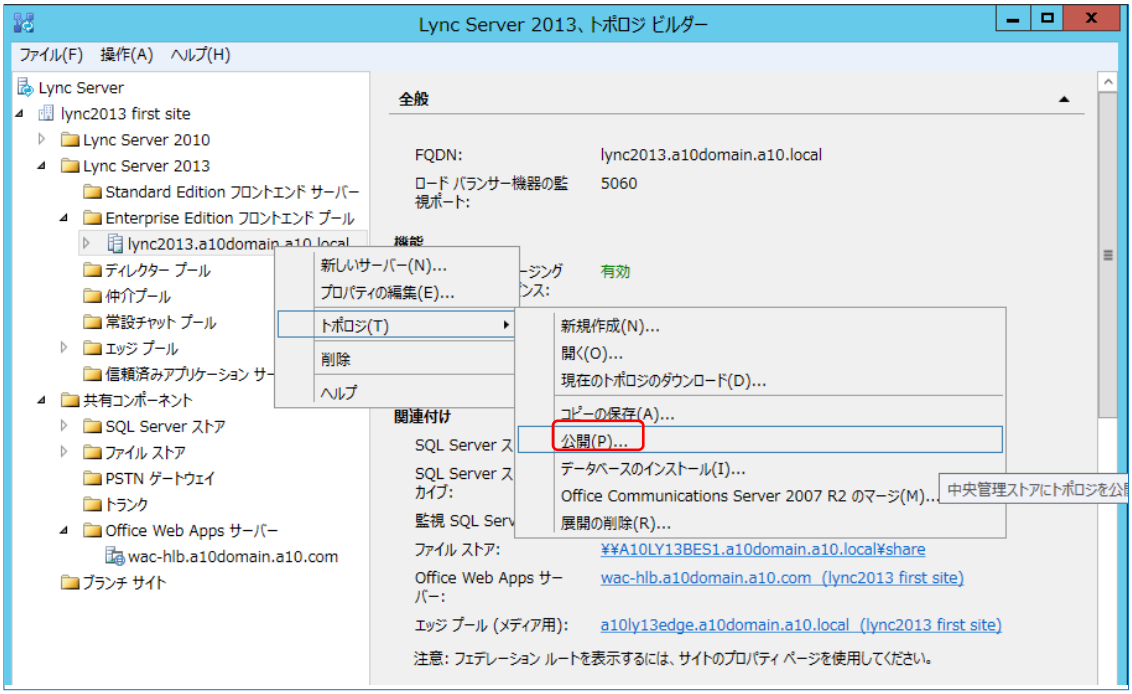

図7：Microsoft Lyncトポロジビルダー

注：トポロジの変更を有効化するために「**公開**」を実行する必要があります。

4 Lync フロントエンドプールのロードバランス

サイトは 1 つまたは複数のプールで構成され、プール内には、1 台または複数の Lync サーバーが含まれます。フロントエンドサーバープールは、Lync サーバーの集合体で、IM/プレゼンス、会議サービス、コラボレーション、音声などのサービスを提供します。プール内の複数サーバーのうち、1 つがダウンしても、残りのフロントエンドサーバーでサービスを継続することができます。

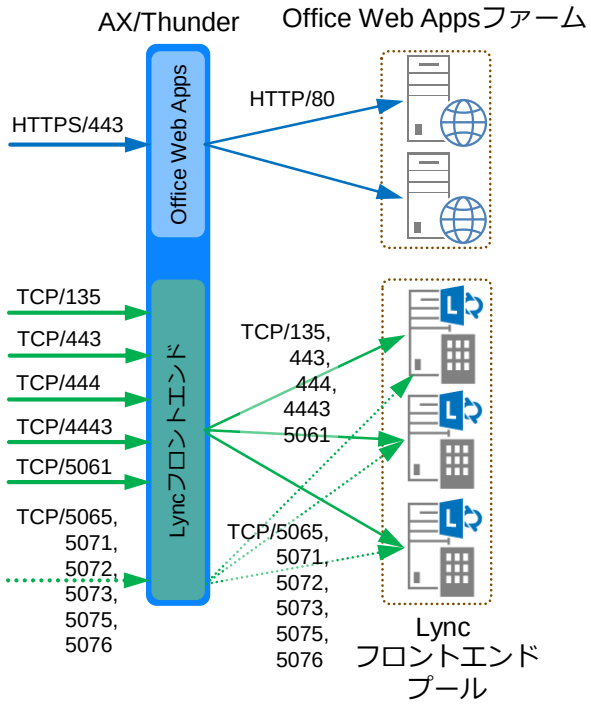

図 8：フロントエンドプール、Office Web Apps 負荷分散構成図

4.1　リアルサーバー設定

ロードバランサを利用して高可用性を構成する Lync フロントエンドエンタープライズプールを、AX/Thunder で設定する手順を以下に記します。

1. **[コンフィグ] > [SLB] > [サービス] > [サーバー]**を選択します。
2. **[追加]**をクリックし、新しいサーバーを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**Lync2013FE1**
   b. [IP アドレス/ホスト]：**192.168.10.17**
   c. [ヘルスモニタ] ：空白 (ヘルスモニタはサービスグループで設定します)

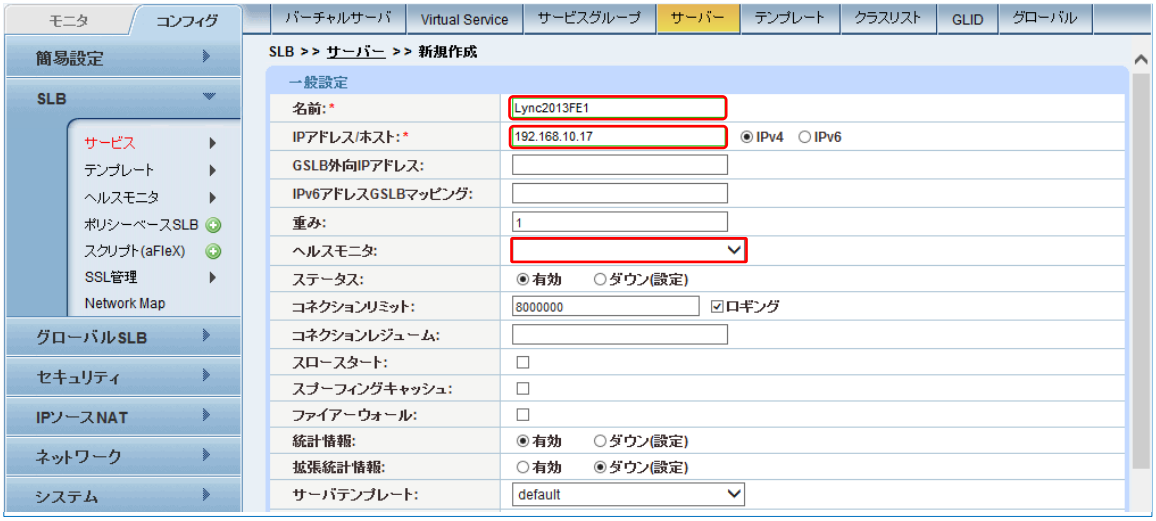

図9：Lyncフロントエンドサーバーの構成

4. 続いてサーバー構成でポートを追加します。
   a. **ポート**を入力、適切な**プロトコル**タイプを選択し、ヘルスチェックを空白にして**[追加]**をクリックします。
   b. 実際に利用するサービスに合わせて、必要なポート設定(表 1 に記載した必須ポートと表 2 に記載したオプションで使用するポート)を全て行います。

注：SSL 通信を利用しないポートを設定する場合には、”SSL なし”をチェックします。

図10：Lyncフロントエンドサーバーポートの構成

5. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
6. 1-4 までの工程を、全フロントエンドサーバー分(今回のケースでは A10LY13FES2, A10LY13FES3)繰り返し実行します。

図 11：Lync フロントエンドサーバー一覧

4.2 サービスグループ設定

続いてサービスグループを構成します。

1. [**コンフィグ**] > [**SLB**] > [**サービス**] > [**サービスグループ**]に移動します。
2. **[追加]**をクリックし、新しいサービスグループを追加します。
3. 今回の構成では、以下の情報を設定しています。
   a. [名前]：**Lync2013SG-135**
   b. [クラス]：**TCP**
   c. [アルゴリズム]：**Least Connection**
   d. [ヘルスモニタ]： **HM**

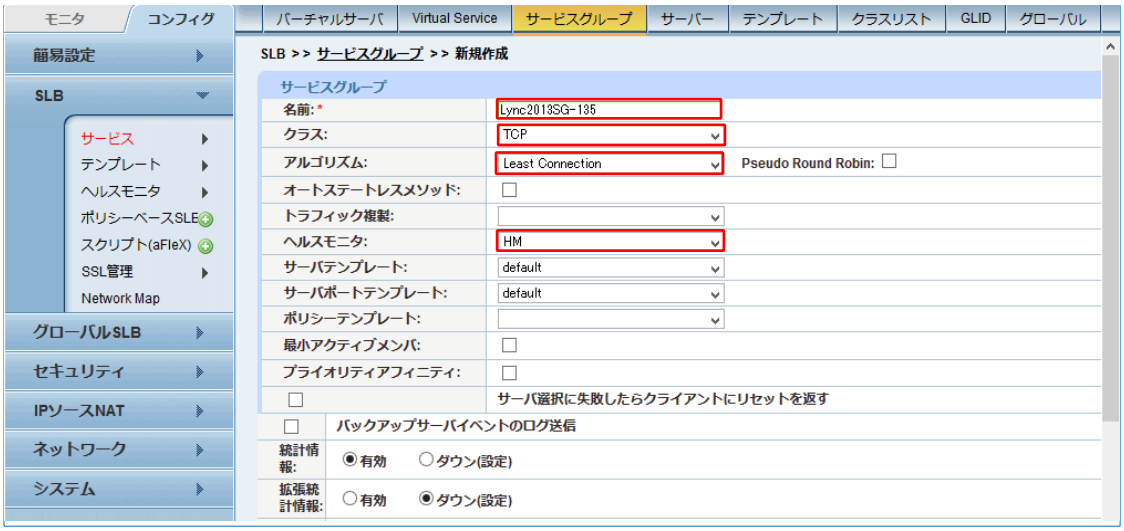

図 12：Lync フロントエンドサービスグループの構成

注：サービスグループは、リアルサーバーとサービスポートのセットで構成され、サーバーの選択アルゴリズムを定義します。

e. [サーバー]ドロップダウンリストから少なくとも 1 つ以上のサーバーを選択してポートと共に追加します。

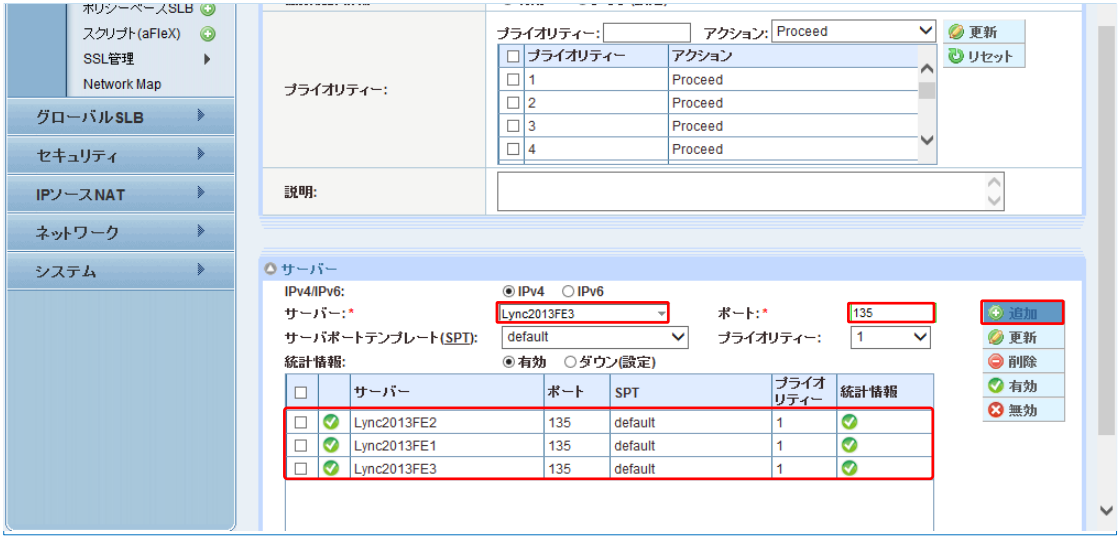

図13： Lyncフロントエンドサービスグループの構成

f. 上記 a-e の工程を、表 1 に記載されている残りの全ポート(TCP/443, TCP/444, TCP/4443, TCP/5061)と必要に応じ、表 2 に記載されているオプションのポート(TCP/5065, TCP/5071, TCP/5072, TCP/5073, TCP/5075, TCP/5076)分実行します。

名前	説明	クラス	ヘルスモニタ	アルゴリズム
Lync2013SG-135		TCP	HM	Least Connection
Lync2013SG-443		TCP	HM	Least Connection
Lync2013SG-444		TCP	HM	Least Connection
Lync2013SG-4443		TCP	HM	Least Connection
Lync2013SG-5061		TCP	HM	Least Connection
Lync2013SG-5065		TCP	HM	Least Connection
Lync2013SG-5070		TCP	HM	Least Connection
Lync2013SG-5071		TCP	HM	Least Connection
Lync2013SG-5072		TCP	HM	Least Connection
Lync2013SG-5073		TCP	HM	Least Connection
Lync2013SG-5075		TCP	HM	Least Connection
Lync2013SG-5076		TCP	HM	Least Connection

図 14：Lync フロントエンドサービスグループ一覧

4.3　バーチャルサーバー設定

1. **[コンフィグ] > [SLB] > [サービス] > [バーチャルサーバー]**に移動します。
2. **[追加]**をクリックし、バーチャルサーバーを追加していきます。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**Lync2013VIP**
   b. [IP アドレス or CIDR Subnet]：**192.168.0.80**

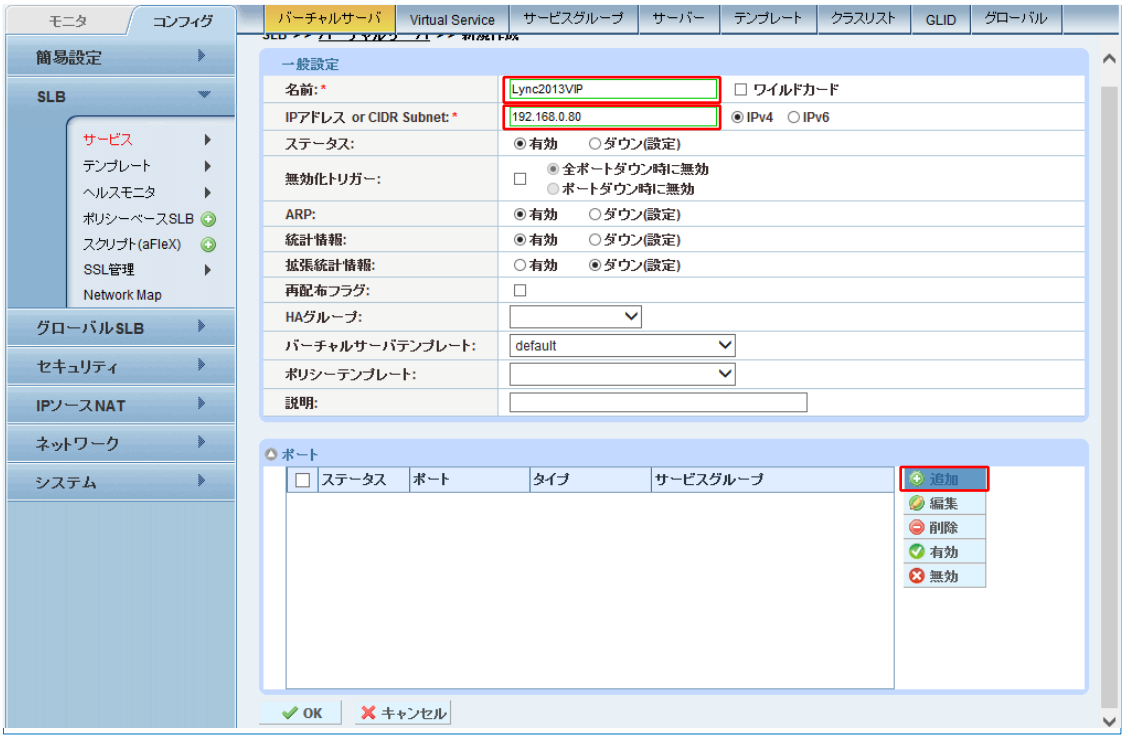

図15：Lyncフロントエンドバーチャルサーバーの構成

注： AX/Thunder上には、複数のバーチャルサーバーを構成できます。バーチャルサーバーは、クライアントの要求送信を受けるサーバーとなります。AX/Thunderは、バーチャルサーバーに紐づくサービスグループから適切なリアルサーバーを選択し、クライアントからの要求を転送処理します。

4. 続いて**ポート**セクションにある**[追加]**をクリックして、バーチャルサービス(バーチャルサーバーポート)を構成します。
5. 本構成では、以下の情報でバーチャルサービス(バーチャルポート)を設定しています。
   a. [タイプ] ：**TCP**
   b. [ポート]：**135**
   c. [サービスグループ]：**Lync2013SG-135**

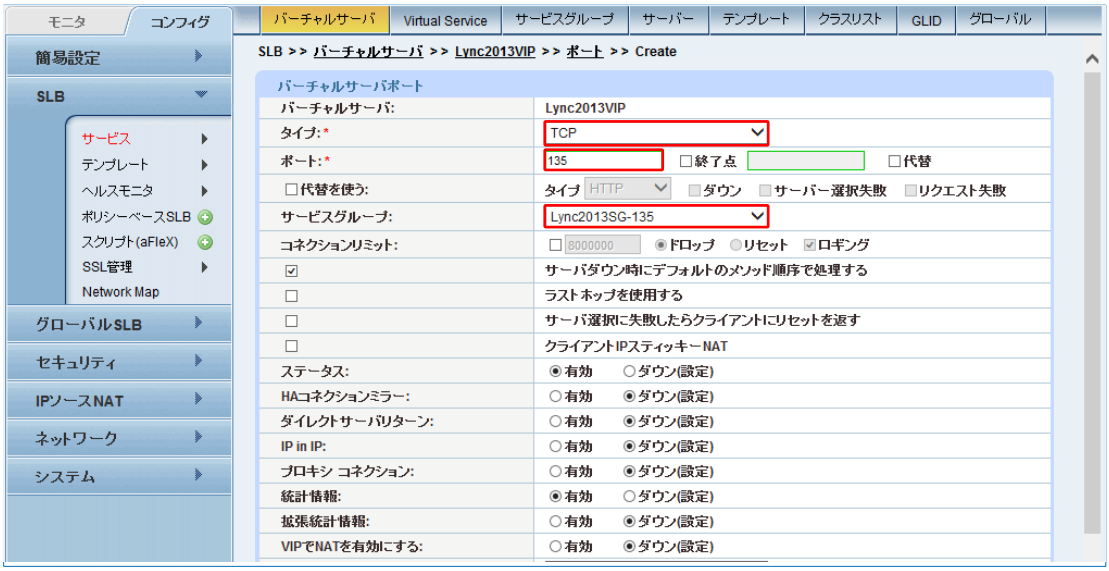

図 16： Lync フロントエンドバーチャルサーバーポートの構成

   d. [ソース NAT プール]： **Auto**

注：本設定で送信元 IP アドレスを、AX/Thunder のサーバー向けネットワークインターフェースに割り当てた IP アドレスに強制的に変更します。

   e. [TCP テンプレート]：**TCP**
   f. [パーシステンステンプレートタイプ]：**ソース IP パーシステンス**
   g. [ソース IP パーシステンス]：**SIP**

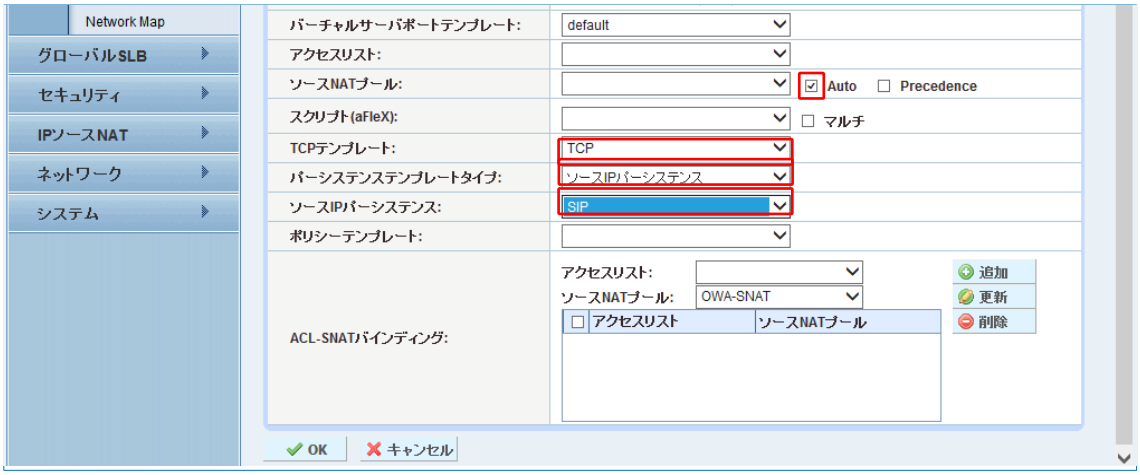

図 17：Lync フロントエンド機能テンプレートの構成

注：各種テンプレートおよびパーシステンスの要件などのAX/Thunderのバーチャルサービステンプレートオプションは、構成要件表に記載されています。**表1**を参照してください。

6. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
7. Lyncフロントエンドサーバーのバーチャルサービスポートの残り分(TCP/443, TCP/444, TCP/4443, TCP/5061)と、利用するサービスに応じてオプションポート(TCP/5065, TCP/5071, TCP/5072, TCP/5073, TCP/5075, TCP/5076)について、3-6の設定を繰り返し実行します。

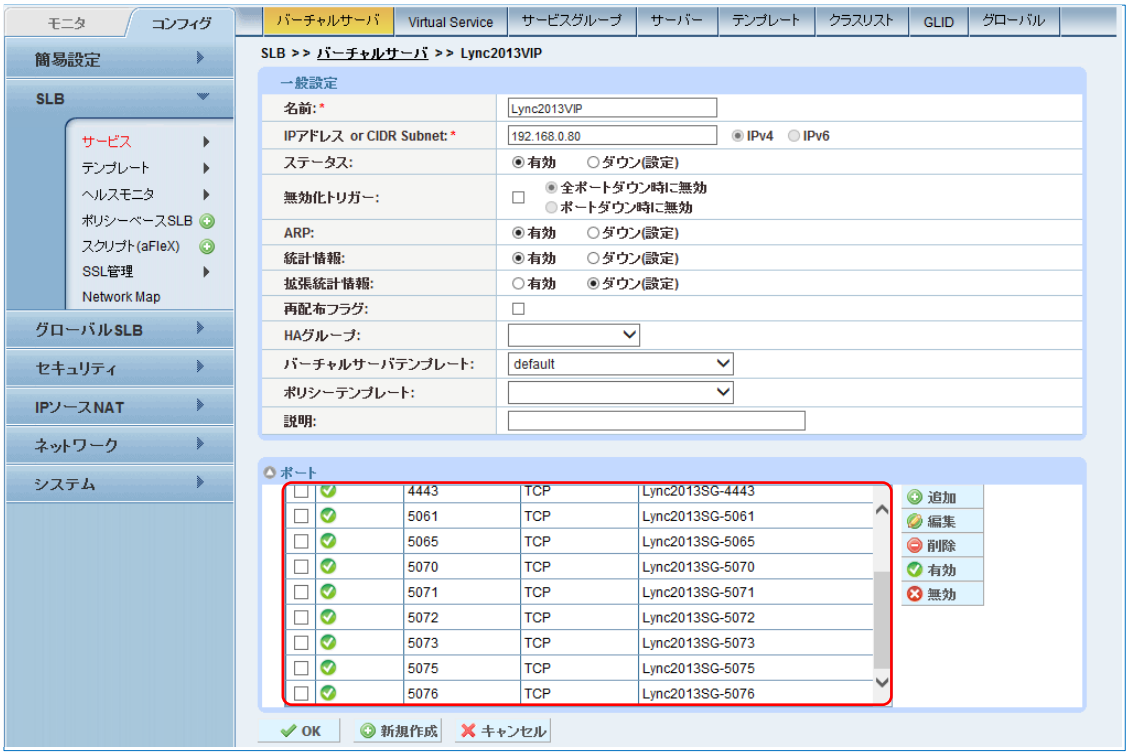

図18：Lyncフロントエンドバーチャルサーバーポートの一覧

8. 最後にバーチャルサーバーの設定画面で、**[OK]**をクリックし、**[保存]**をクリックして構成を保存します。

5 外部エッジプールのロードバランス

エッジサーバーは、外部ユーザが企業のファイアウォールを越えて Lync サーバーにアクセスすることを可能にします。エッジサーバーを設置することで、リモートユーザは、IM/プレゼンス、会議並びに音声機能を VPN 接続無しで利用できます。さらに、エッジサーバーを設置することで、他企業とのフェデレーションやパブリック IM 接続なども実現することができ、ユーザは豊富な Lync 機能を全て利用することができます。エッジサーバーは、単一サーバーまたは複数サーバーのどちらでも展開できます。ロードバランサは、アプリケーションに冗長性と 復元性を提供する複数サーバー展開時に必要となります。

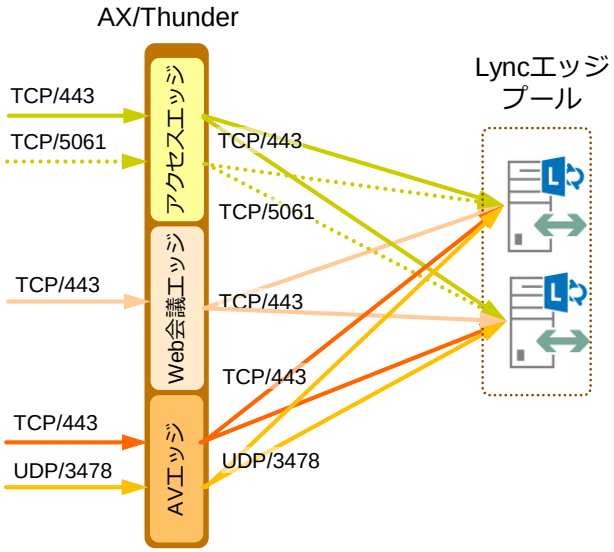

図 19：外部エッジ向け負荷分散構成図

5.1 リアルサーバー設定

Lync 外部エッジプールを構成する方法を以下に記します。

1. **[コンフィグ] > [SLB] > [サービス] > [サーバー]**に移動します。
2. **[追加]**をクリックし、新しいサーバーを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**ExternalEdge1-access**
   b. [IP アドレス/ホスト]：**172.17.0.21**
   c. [ヘルスモニタ]：**空白** (ヘルスモニタはサービスグループで構成します)

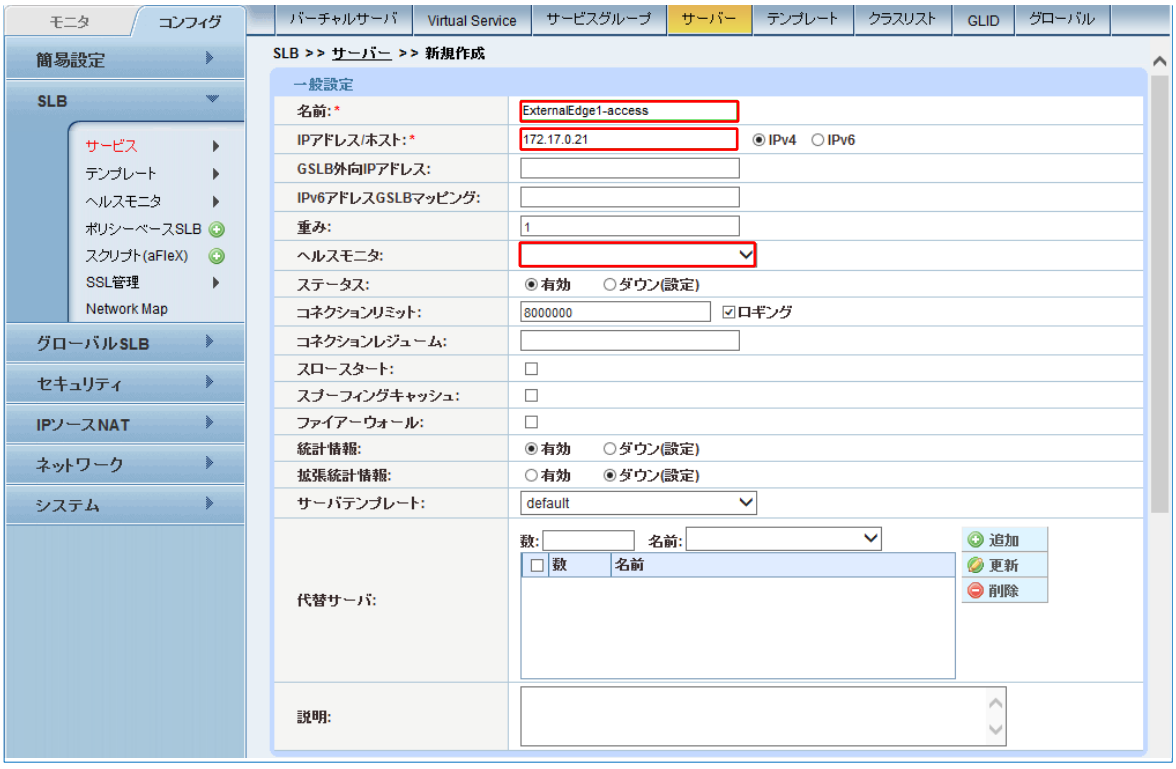

図 20：外部エッジサーバーの構成

4. **ポート**セクションで**[追加]**を選択します。
5. 必要なポート情報(表 4 に記載)を追加し、**[OK]**をクリックした後、**[保存]**をクリックして構成を保存します。

   ヘルスモニタはサービスグループで設定するため、ここでは空白を選択します。

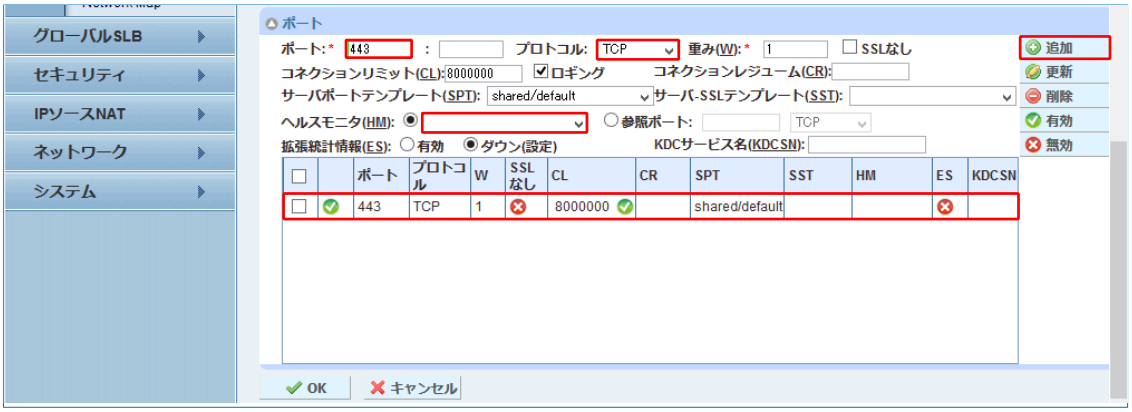

図 21：外部エッジサーバーポートの構成

注：外部エッジサービスの必須ポートについては、**表4**を参照してください。今回のケースでは、アクセス、Web会議、AVエッジのIPアドレスは各々独立しており同じポート番号443を利用しています。

6. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
7. 1-5 までの工程を、全ての外部エッジサーバー分(A10LY13EGS1 の Web 会議エッジ、AV エッジ並びに A10LY13EGS2 の全エッジ)について、繰り返し実行します。

図 22：外部エッジサーバー一覧

5.2 サービスグループ設定

1. **[コンフィグ] > [SLB] > [サービス] > [サービスグループ]**を選択します。
2. **[追加]**をクリックし、新しいサービスグループを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**ExternalEdge-access-443**
   b. [クラス]：**TCP**
   c. [アルゴリズム]：**Least Connection**
   d. [ヘルスモニタ]：**HM**

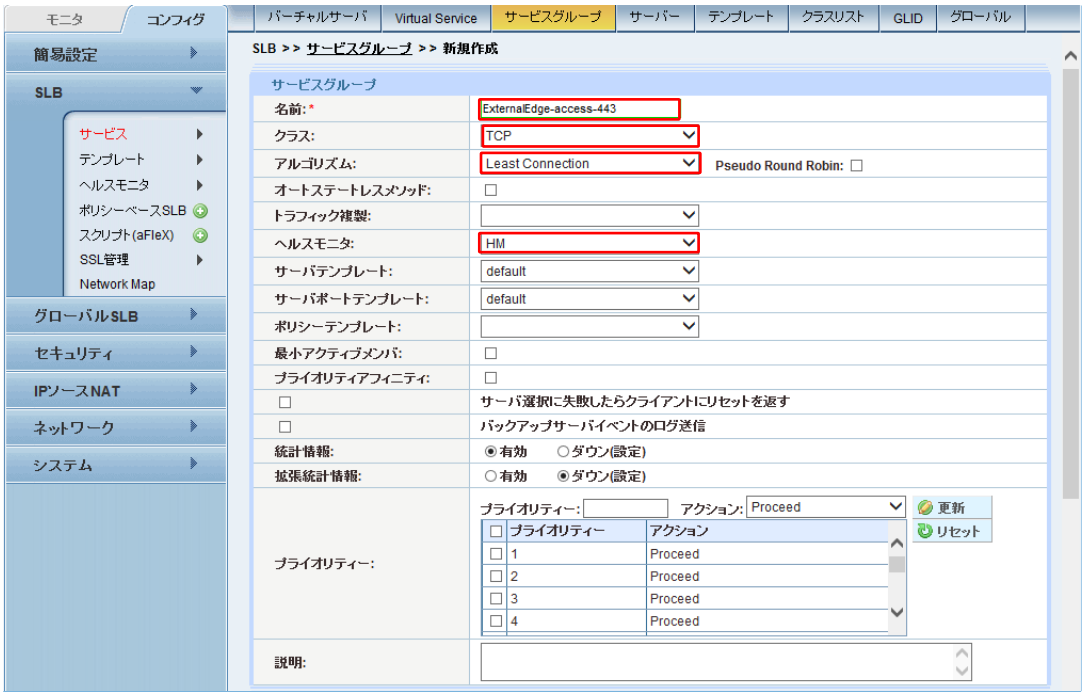

図 23：外部エッジサービスグループの構成

注：サービスグループは、リアルサーバーとサービスポートのセットで構成され、サーバーの選択アルゴリズムを定義します。

4. **[サーバー]**ドロップダウンリストから少なくとも 1 つ以上のサーバーを選択してポートと共に追加します。

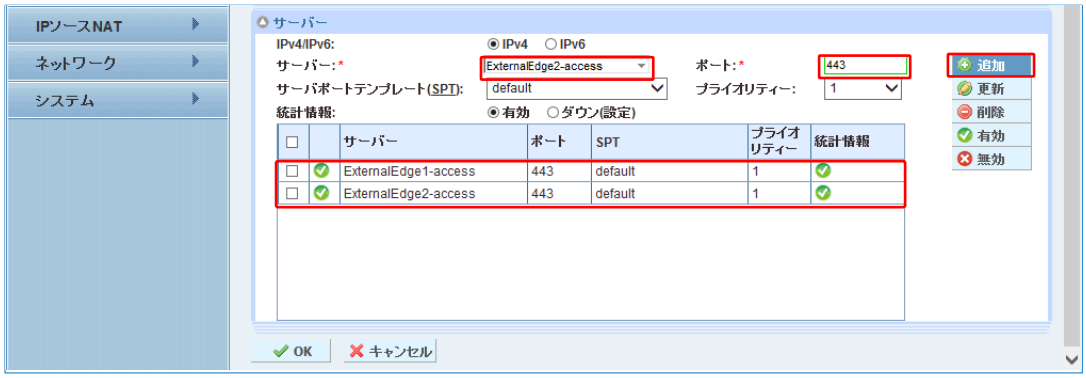

図24：外部エッジサービスグループサーバーの一覧

5. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
6. 外部エッジサービスに必須のサービスグループ（表 4 に記載）すべてについて、上記の 1-4 の設定を繰り返し実施します。

名前	説明	クラス	ヘルスモニタ	アルゴリズム
ExternalEdge-access-443		TCP	HM	Least Connection
ExternalEdge-access-5061		TCP	HM	Least Connection
ExternalEdge-av-3478		UDP	HM	Least Connection
ExternalEdge-av-443		TCP	HM	Least Connection
ExternalEdge-web-443		TCP	HM	Least Connection

図25：外部エッジサービスグループ一覧

注：フェデレーション接続、パブリックIM接続が無いケースでは、外部アクセスエッジのTCP/5061を構成する必要はありません。今回のテスト環境では接続先はありませんが、設定だけ実施しております。

5.3　バーチャルサーバー設定

前章のフロントエンドサーバーのバーチャルサーバーでは、明示的にバーチャルサーバーとバーチャルサーバーポートの設定を分ける方法を記載しましたが、外部エッジのバーチャルサーバーは、バーチャルサービス(バーチャルサーバーポート)の設定の一環で定義します。
どちらの方法でも、設定内容は完全に一致しており、特に問題ありません。
本構成では、アクセスエッジ、Web エッジ、AV エッジのパブリック(公開)IP アドレス(VIP)が独立していますので、アクセスエッジ以外の 2 つのエッジ役割向けに、下記のバーチャルサービスの設定を繰り返し実行する必要があります

1.
2. **[コンフィグ] > [SLB] > [サービス] > [バーチャルサービス]**に移動します。
3. **[追加]**ボタンをクリックし、バーチャルサービスを追加します。
4. 本構成では、以下の情報を設定してします。
    a. [バーチャルサービス]：**ExternalEdge-ac443**
    b. [タイプ]：**TCP**
    c. [ポート]：**443**
    d. [アドレス]：**172.17.0.111**
    e. [サービスグループ]：**ExternalEdge-access-443**

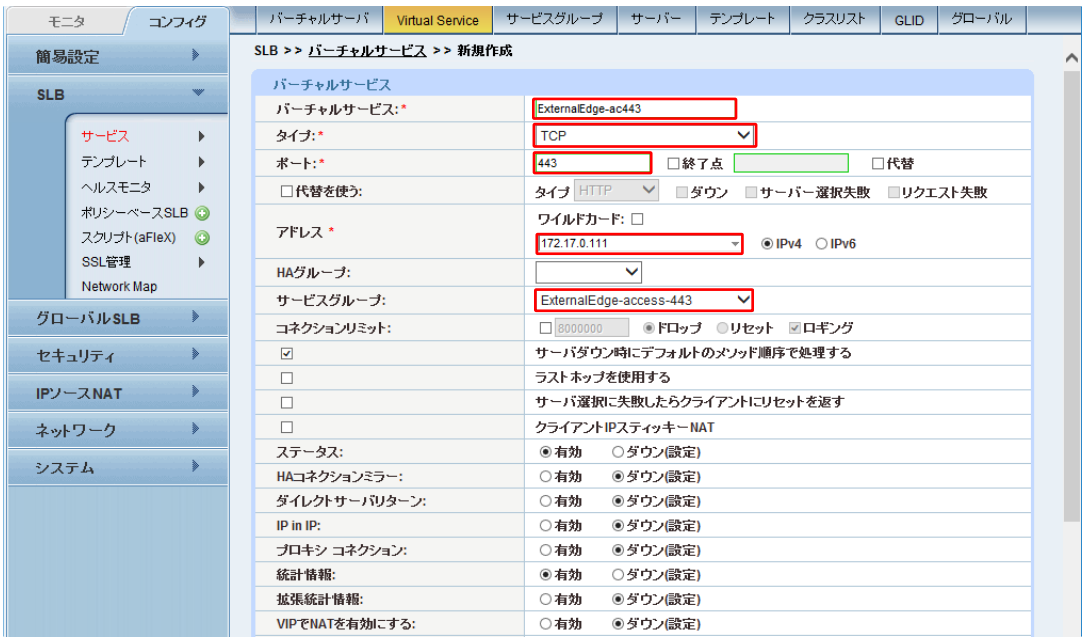

図 26：外部エッジバーチャルサービスの構成

機能テンプレートとして以下を構成します

a. [ソース NAT プール]：**Auto**

b. [TCP テンプレート]：**TCP**

c. [パーシステンステンプレートタイプ]：**ソース IP パーシステンス**

d. [ソース IP パーシステンス]：**SIP**

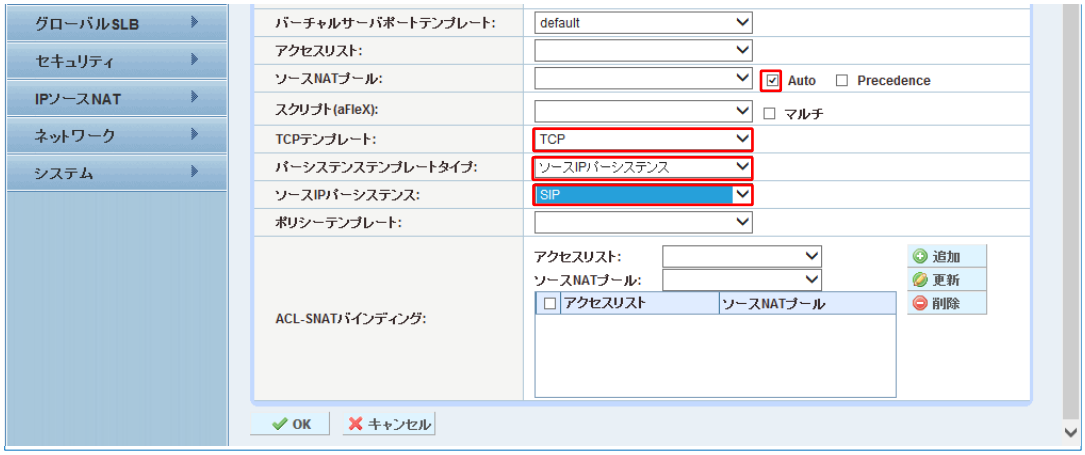

図 27：外部エッジバーチャルサービス機能テンプレート

注：各種テンプレートおよびパーシステンスの要件などを含むAX/Thunderのバーチャルサービステンプレートオプションは、構成要件表に記載されています。**表4**を参照してください。

1. 完了したら、**[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
2. 1-3の工程を、表4で記載されているWeb会議エッジとAVエッジのバーチャルサーバーとバーチャルサービスポート (TCP/443、UDP/3478)に対して実行します。

注：アクセスエッジのTCP/5061については、今回の構成で利用していないため定義しておりません。

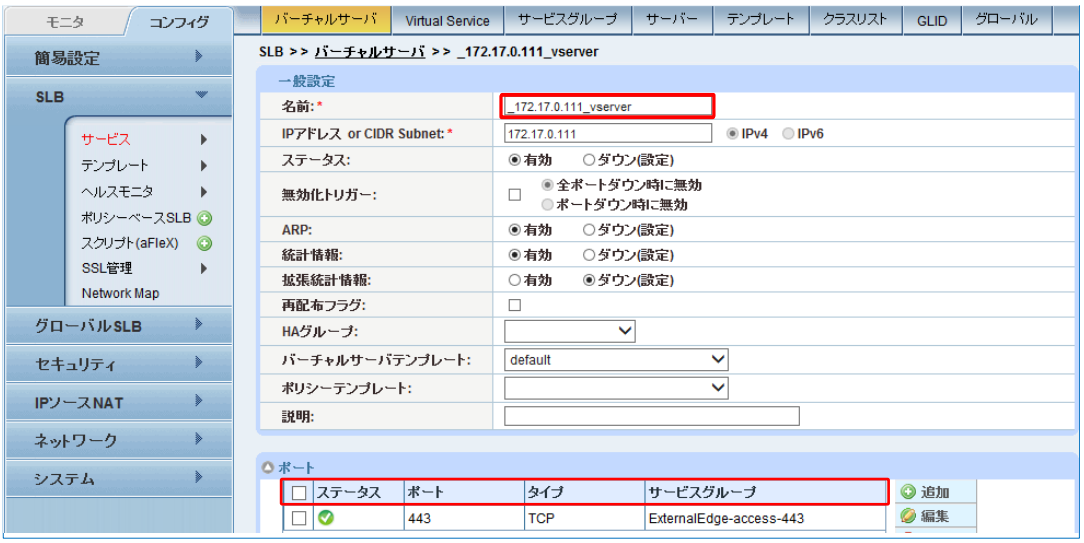

図 28：外部アクセスエッジバーチャルサーバーの構成

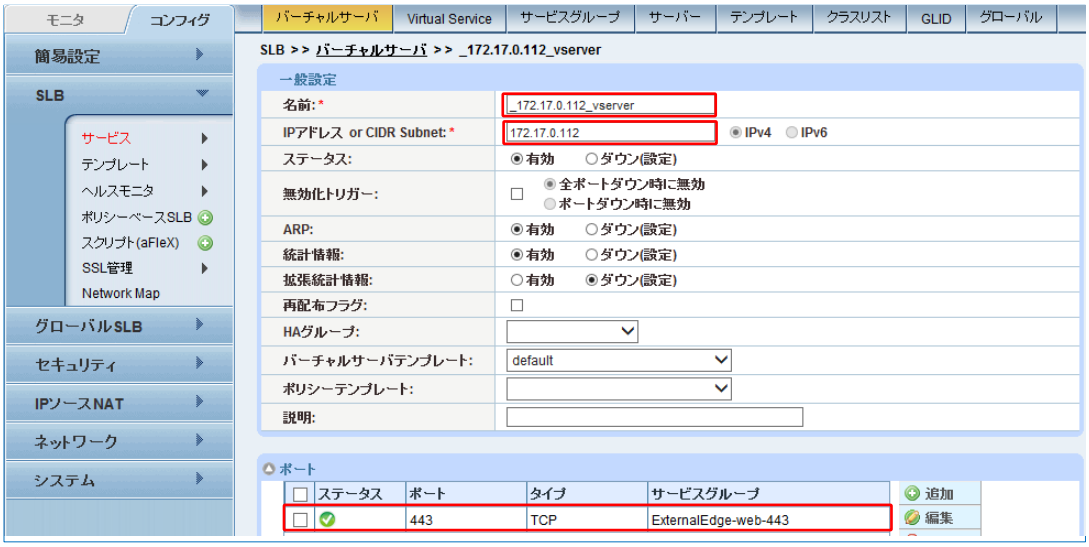

図 29：外部 Web エッジバーチャルサーバーの構成

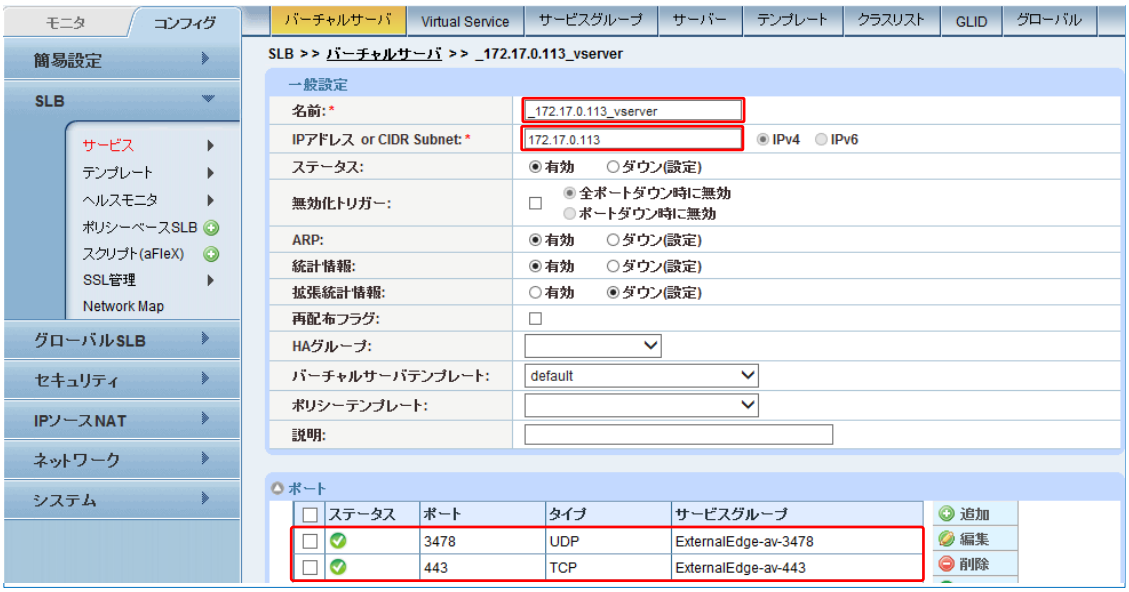

図 30：外部 Web エッジバーチャルサーバーの構成

6 内部エッジプールのロードバランス

外部エッジプールの負荷分散として専用のロードバランサ(AX/Thunder)を利用した場合には、内部エッジプールでも同様のロードバランサが必須となります。外部エッジプールに DNS ロードバランスを利用した場合には、内部エッジプールでも DNS ロードバランスを使用することが要求されます。内部エッジプールでは、Lync サーバー若しく内部ネットワークの Lync クライアントから外部ネットワークの Lync クライアントや他 Lync システムへの通信を処理します。内部エッジプールは、外部エッジプール(アクセスエッジ、Web 会議エッジ、AV エッジ)と違いサーバー役割は単一です。

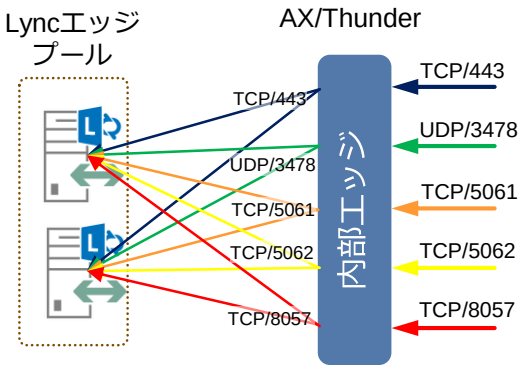

図 31：内部エッジ向け負荷分散構成図

AX/Thunder で Lync 内部エッジプールを構成する方法を、以降に記します。

6.1 リアルサーバー設定

1. **[コンフィグ] > [SLB] > [サービス] > [サーバー]**に移動します。
2. **[追加]**をクリックし、内部エッジサーバーを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**InternalEdge-1**
   b. [IP アドレス/ホスト]：**172.19.0.121**
   c. [ヘルスモニタ] : **空白** (ヘルスモニタはサービスグループで設定します)

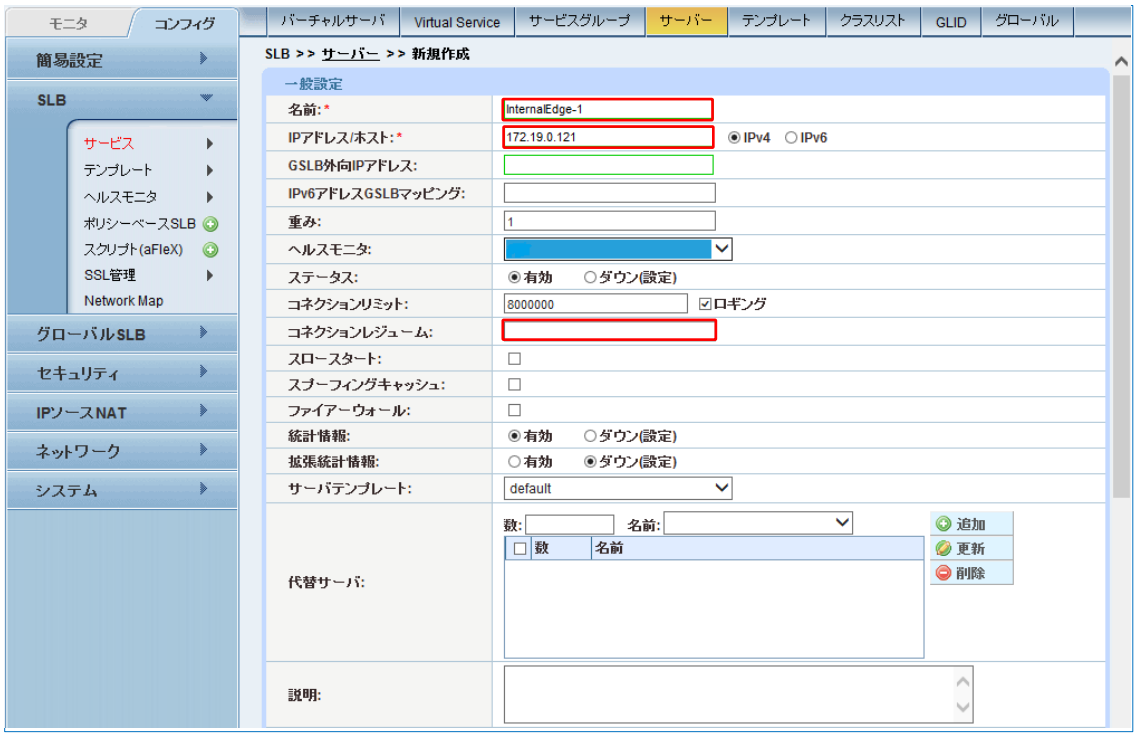

図32：内部エッジサーバーの構成

4. **[ポート]**セクションにある**[追加]**を選択し、サーバー構成にポートを追加します。

   a. **ポート**および**プロトコル**タイプを入力し、ヘルスモニタを空白にして**[追加]**をクリックします。

   b. 実際に利用するサービスに合わせて、必要なポートの設定を実行します。

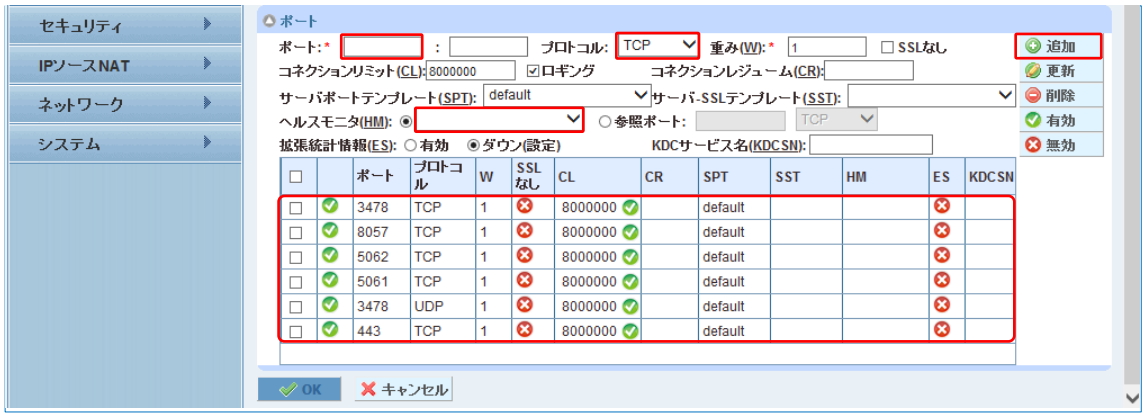

図33：内部エッジサーバーポートの構成

注：内部エッジサービスの必須ポートについては、**表3**を参照してください。

5. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。

6. 1-4 までの工程を、残りの全ての内部エッジサーバー (本構成では A10LY13EGS2) について、繰り返し実行します。

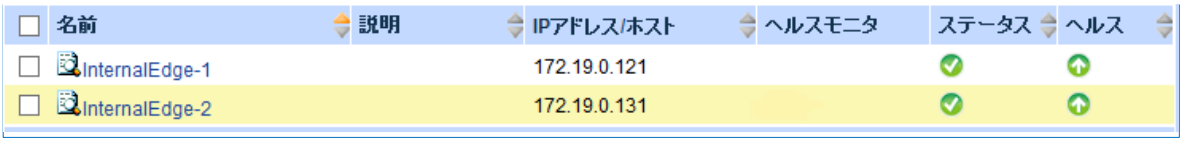

図34：内部エッジサーバー一覧

6.2 サービスグループ設定

1. **[コンフィグ] > [SLB] > [サービス] > [サービスグループ]**に移動します。
2. **[追加]**をクリックし、新しいサービスグループを作成します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**internalEdge-443**
   b. [クラス]：**TCP**
   c. [アルゴリズム]：**Least Connection**
   d. [ヘルスチェック]：**HM**

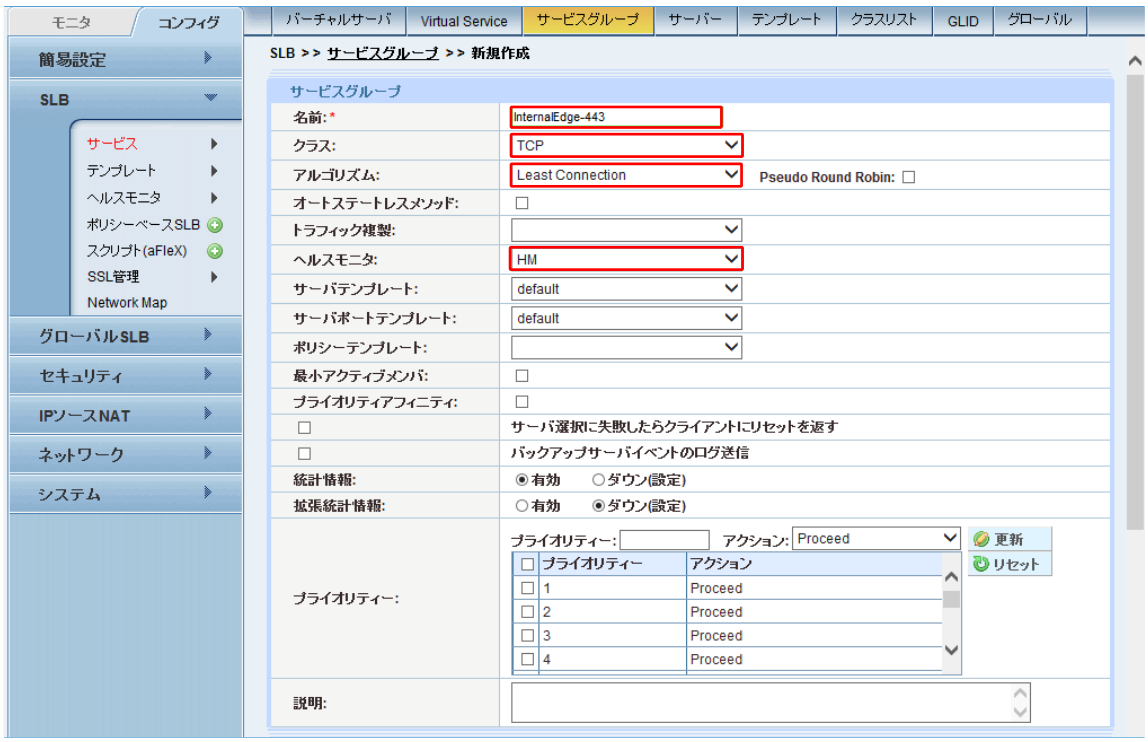

図35：内部エッジサービスグループの構成

注：サービスグループは、リアルサーバーとサービスポートのセットで構成され、サーバーの選択アルゴリズムを定義します。

e. [サーバー]ドロップダウンリストから少なくとも 1 つ以上のサーバーを選択してポートと共に追加します。

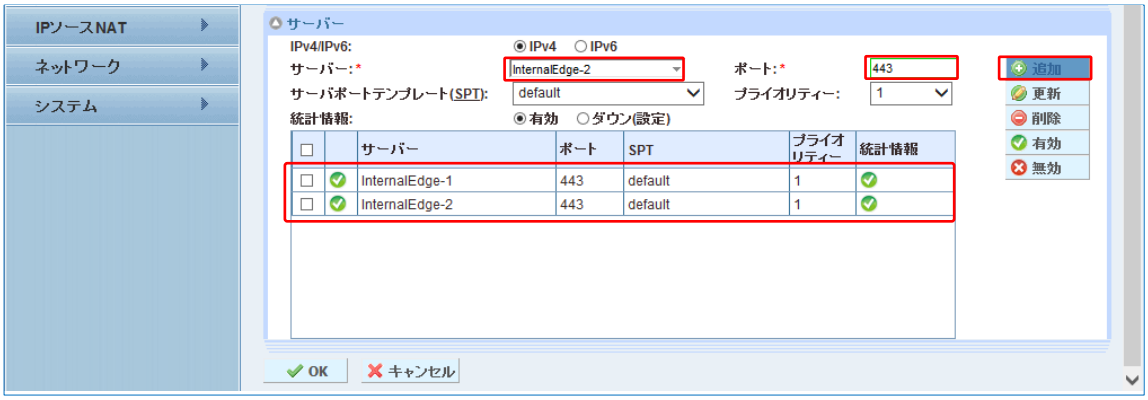

図 36：内部エッジサービスグループのサーバー一覧

f. 上記 a-e の工程を、表 3 に記載されている残りの TCP ポート分(TCP/5061, TCP/5062, TCP/8057)全てに対して実行します。
UDP/3478 は設定内容が異なるため、次に設定例を記します。

図 37：内部エッジサービスグループ一覧

4. 下記は、UDP/3478 をサービスグループで定義した内容です。

   a. [名前]： **InternalEdge-3478**

   b. [クラス] ： **UDP**

   c. [アルゴリズム] ：**Least Conenction**

   d. [ヘルスモニタ] ： **HM**

   e. [サーバー] ： **InternalEdge-1, InternalEde-2**

   f. [ポート] ： **3478**

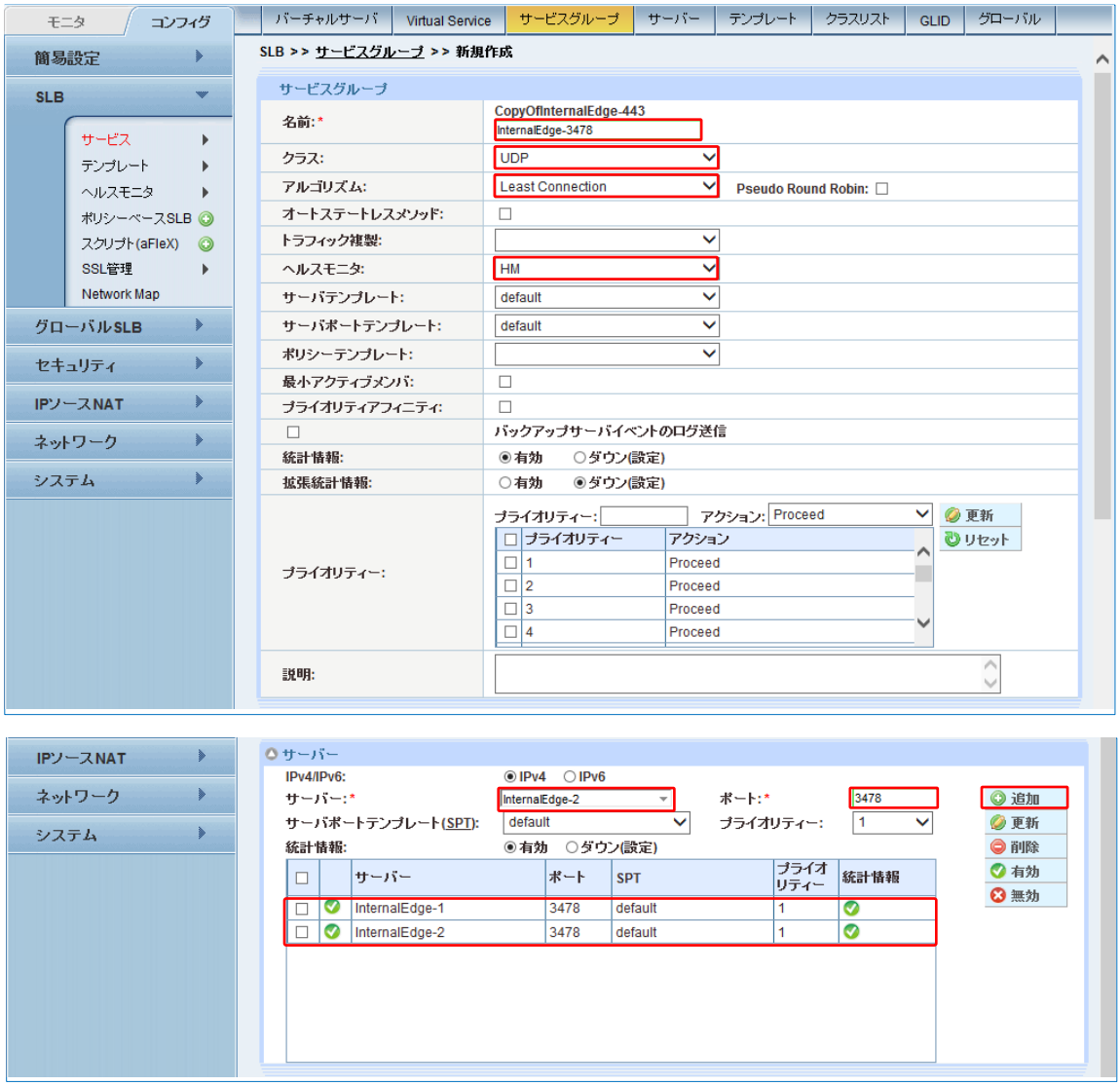

図 38：UDP/3478 のサービスグループ設定

6.3　バーチャルサーバー設定

内部エッジのバーチャルサーバーは、外部エッジ同様バーチャルサービスの設定の一環で定義します。

1. **[コンフィグ]** > **[SLB]** > **[サービス]** > **[バーチャルサービス]**に移動します。
2. **[追加]**ボタンをクリックし、バーチャルサービスを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [バーチャルサービス]：**Internal-443**
   b. [タイプ]：**TCP**
   c. [ポート]：**443**
   d. [アドレス]：**172.19.0.101**
   e. [サービスグループ]：**InternalEdge-443**

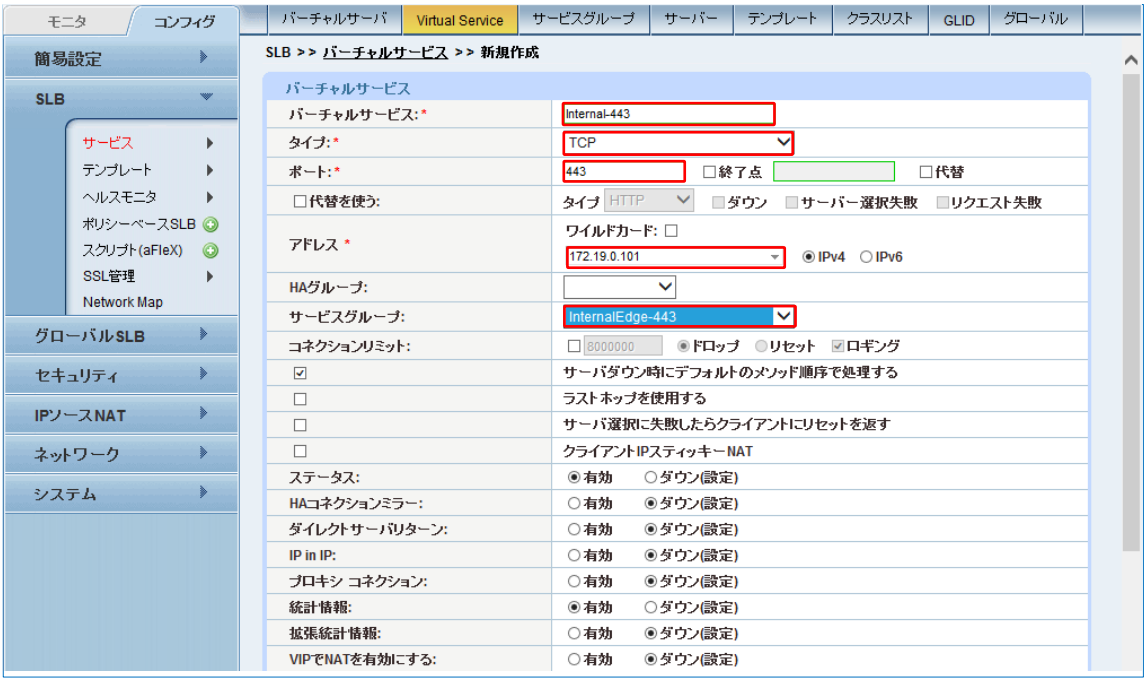

図39：内部エッジバーチャルサービスの構成

機能テンプレートとして以下を構成します

f. [ソース NAT プール]：**Auto**

g. [TCP テンプレート] : **TCP**

h. [パーシステンステンプレートタイプ] ： **ソース IP パーシステンス**

i. [ソース IP パーシステンス] ： **SIP**

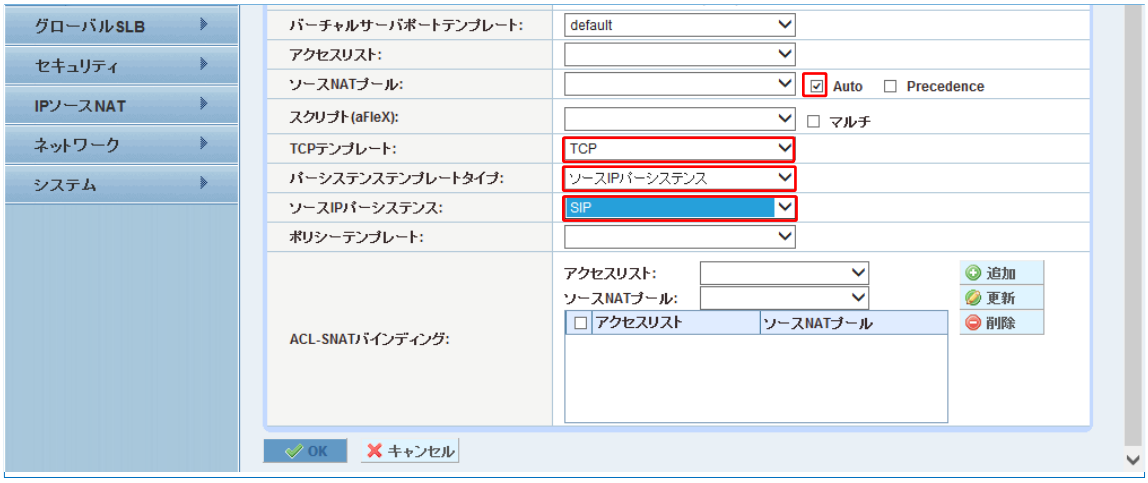

図 40：内部エッジバーチャルサービス機能テンプレートの構成

注：各種テンプレートおよびパーシステンスの要件を含むAX/Thunderのバーチャルサービステンプレートオプションは、構成要件表に記載されています。**表3**を参照してください。

4. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。

5. 上記 1-3 の工程を、表 3 の残りのポート分(UDP/3478, TCP/5061, TCP/5062, TCP/8057)全てに対して実行します。設定する VIP アドレス、サービスグループ、機能テンプレートは UDP/3478 を除き全て共通となります。

C. 以下は、UDP/3478 の設定内容となります。

1. 本構成では下記内容で設定を実施しています。

a. [バーチャルサービス]：**Internal-3478-UDP**

b. [タイプ]：**UDP**

c. [ポート] : **3478**

d. [アドレス] : **_172.19.0.101_vserver**

(既に同 IP アドレスの設定があるためリストから選択する形となります)

e. [サービスグループ] : **InternalEdge-3478**

f. [ソース IP パーシステンス] ： **SIP**

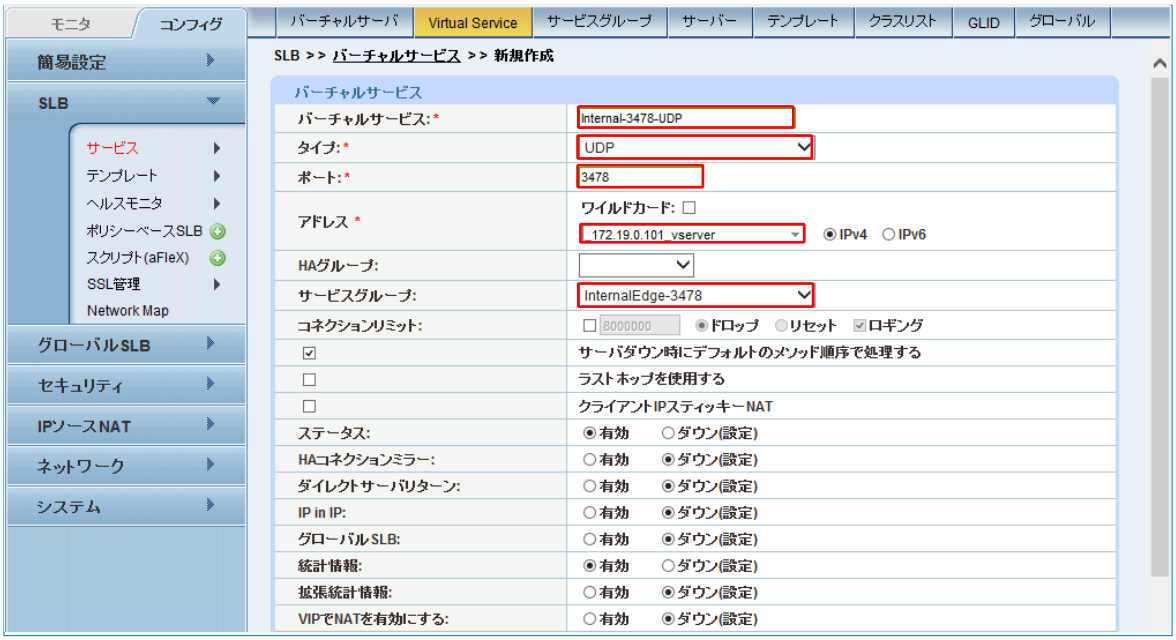

図 41：UDP/3478 のバーチャルサービスの構成

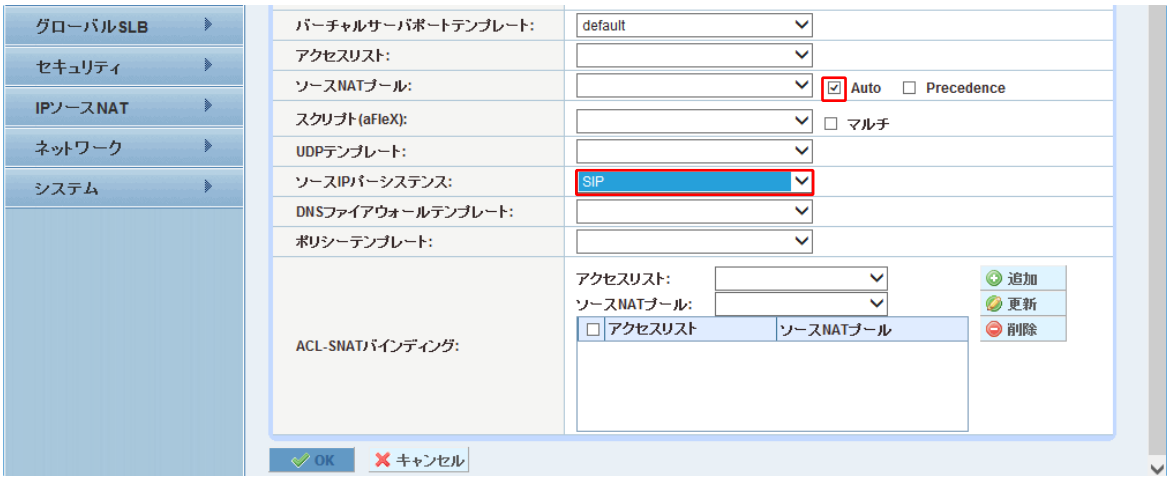

図 42：UDP/3478 バーチャルサービス機能テンプレートの構成

注：各種テンプレートおよびパーシステンスの要件を含むAX/Thunderのバーチャルサービステンプレートオプションは、構成要件表に記載されています。**表3**を参照してください。

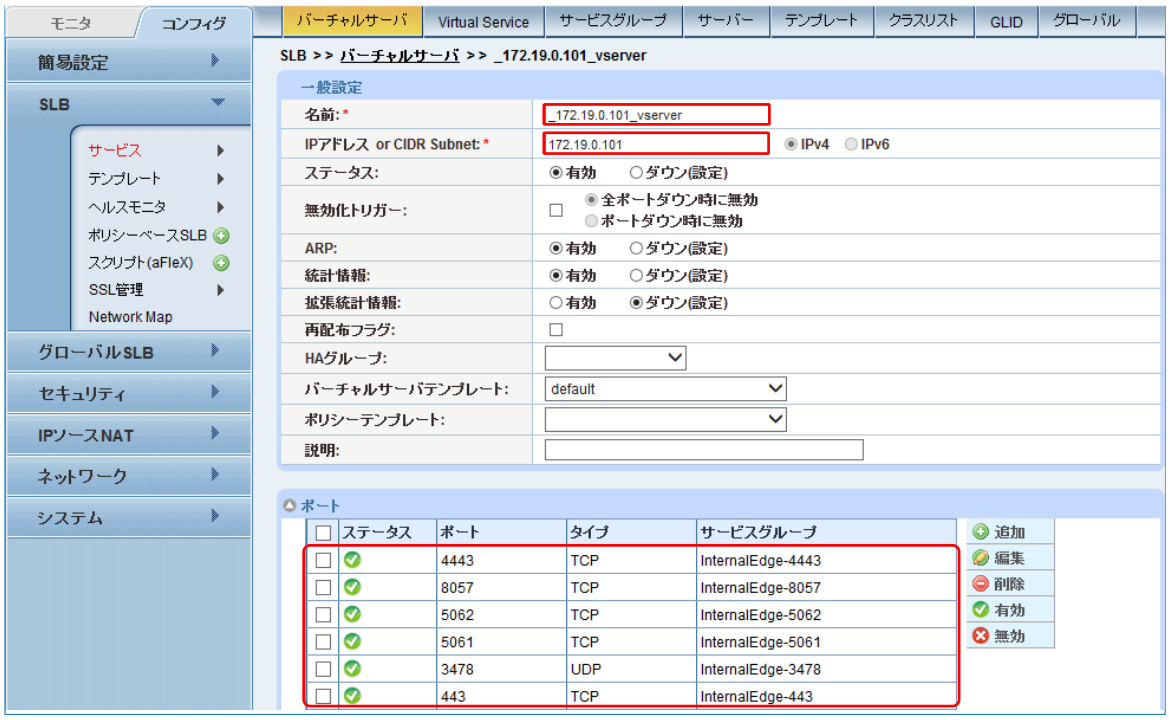

図43：内部エッジバーチャルサーバーの構成

注：内部エッジサービスで定義する必須ポートのリストについては、**表 3** を参照してください。

7 Office Web Apps ファームのロードバランス

AX/Thunder で Office Web Apps プールを構成する方法を記します。Office Web Apps サーバーのロードバランス要件で SSL オフロードを推奨しているため、以下では SSL オフロードの構成方法を記載します。なお、その他サーバー負荷軽減機能(RAM キャッシング、圧縮等)も有効ですが、本構成では設定しておりません。

負荷分散構成イメージについては、"図 8：フロントエンドプール向け負荷分散構成図”にまとめて記載しています。

7.1 リアルサーバー設定

1. **[コンフィグ] > [SLB] > [サービス] > [サーバー]**に移動します。
2. **[追加]**をクリックし、Office Web Apps サーバーを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**WAC1**
   b. [IP アドレス/ホスト]：**192.168.10.23**
   c. [ヘルスモニタ] : **空白** (ヘルスモニタはサービスグループで設定します)

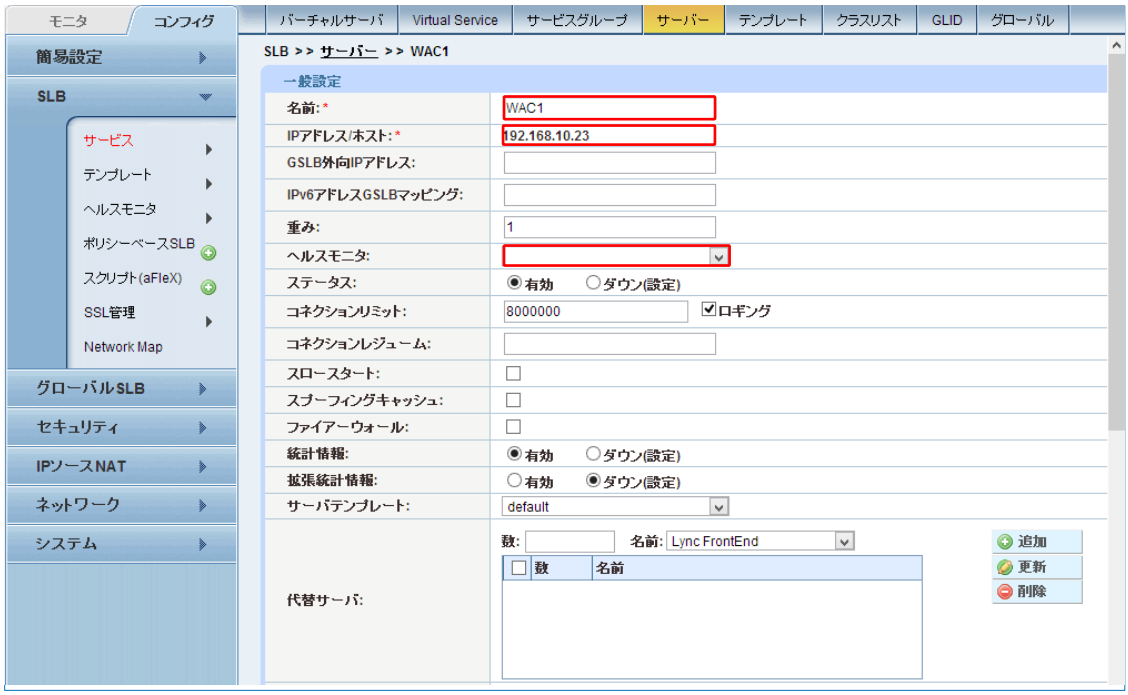

図44：Office Web Appsサーバーの構成

4. **[ポート]**セクションにある**[追加]**を選択し、サーバー構成にポートを追加します。
   a. ポート **80** を入力、プロトコルタイプで **TCP** を選択、SSL なしをチェックし、**[追加]**をクリックします。
   b. ポート **443** を入力、プロトコルタイプで **TCP** を選択し、**[追加]**をクリックします。

図45：Office Web Appsサーバーポートの構成

注 : SSL オフロードを構成する場合には、TCP/443 の設定は本来不要ですが、本構成では SSL オフロード無のテストも実施したため、両方設定しております。

5. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
6. 1-4 までの工程を、残り全ての Office Web Apps サーバー分(本構成では A10LY13WAC2)について、繰り返し実行します。

7.2 サービスグループ設定

1. **[コンフィグ] > [SLB] > [サービス] > [サービスグループ]**に移動します。
2. [追加]をクリックし、[**WAC-SG-80**」という新しいサービスグループを作成します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**WAC-SG-80**
   b. [クラス]：**TCP**
   c. [アルゴリズム]：**Least Connection**
   d. [ヘルスモニタ]：**WAC-80**　(構成については後述)

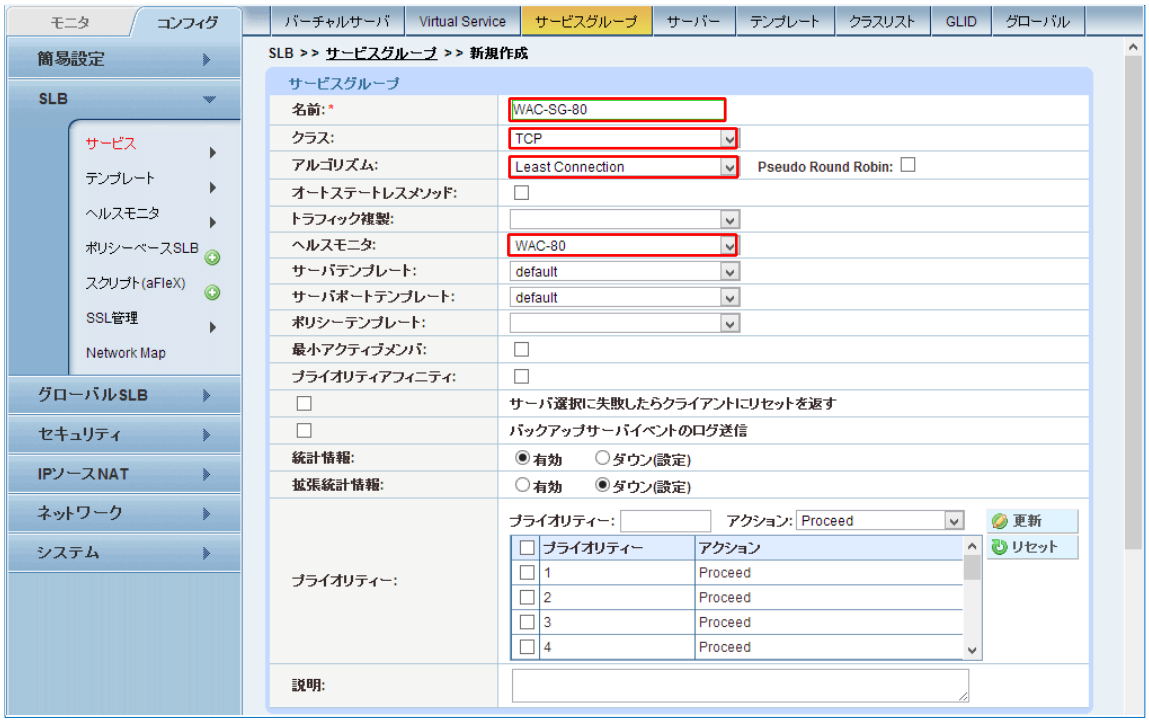

図46：Office Web Appsサービスグループの構成

注：サービスグループは、リアルサーバーとサービスポートのセットで構成され、サーバーの選択アルゴリズムを定義します。

e. [サーバー]ドロップダウンリストから少なくとも 1 つ以上のサーバーを選択してポートと共に追加します。本構成では、サーバー名 **WAC1** および **WAC2** をポート **80** で設定しています。

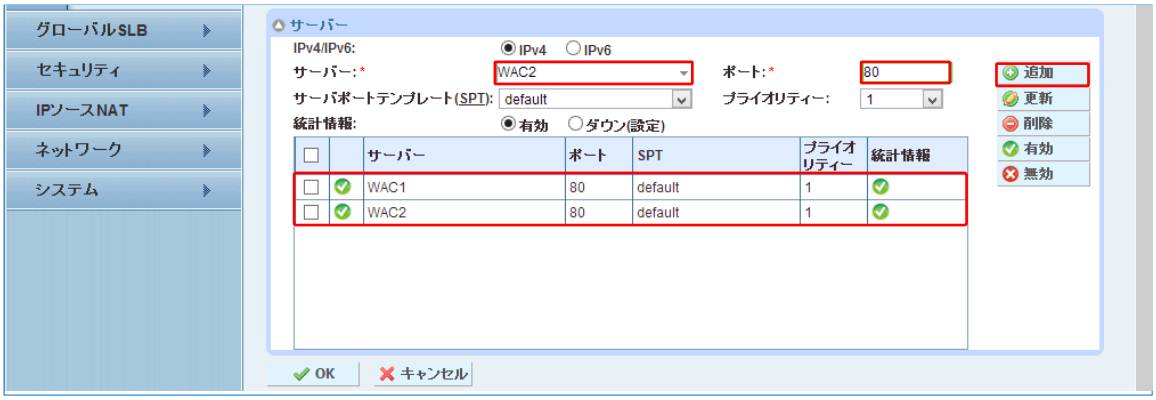

図 47：Office Web Apps サービスグループのサーバー一覧

4. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

7.3　バーチャルサーバー設定

Office Web Apps のバーチャルサーバーは、外部エッジ、内部エッジ同様バーチャルサービスの設定の一環で定義します。

1. **[コンフィグ]** > **[SLB]** > **[サービス]** > **[バーチャルサーバーポート]**に移動します。
2. **[追加]**ボタンをクリックします。
3. 本構成では、以下の情報を設定しています。
   a. [バーチャルサービス]：**OWA_VIP**
   b. [タイプ]：**https**
   c. [ポート]：**443**
   d. [アドレス]：**192.168.10.86**
   e. [サービスグループ]：**WAC-SG-80**

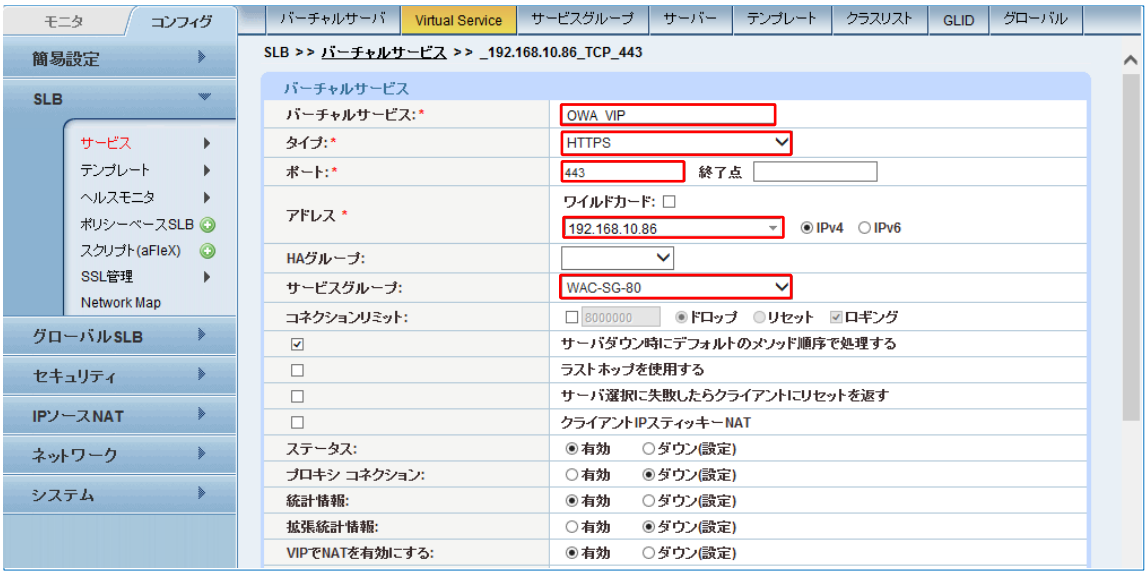

図 48：Office Web Apps バーチャルサービスの構成

機能テンプレートとして以下を構成します

f. [ソース NAT プール]：**Auto**

g. [クライアント SSL テンプレート] : **wac-hlb-c-ssl** (構成については後述)

h. [パーシステンステンプレートタイプ] ： **クッキーパーシステンステンプレート**

i. [クッキーパーシステンステンプレート] ： **persistence-wac** (構成については後述)

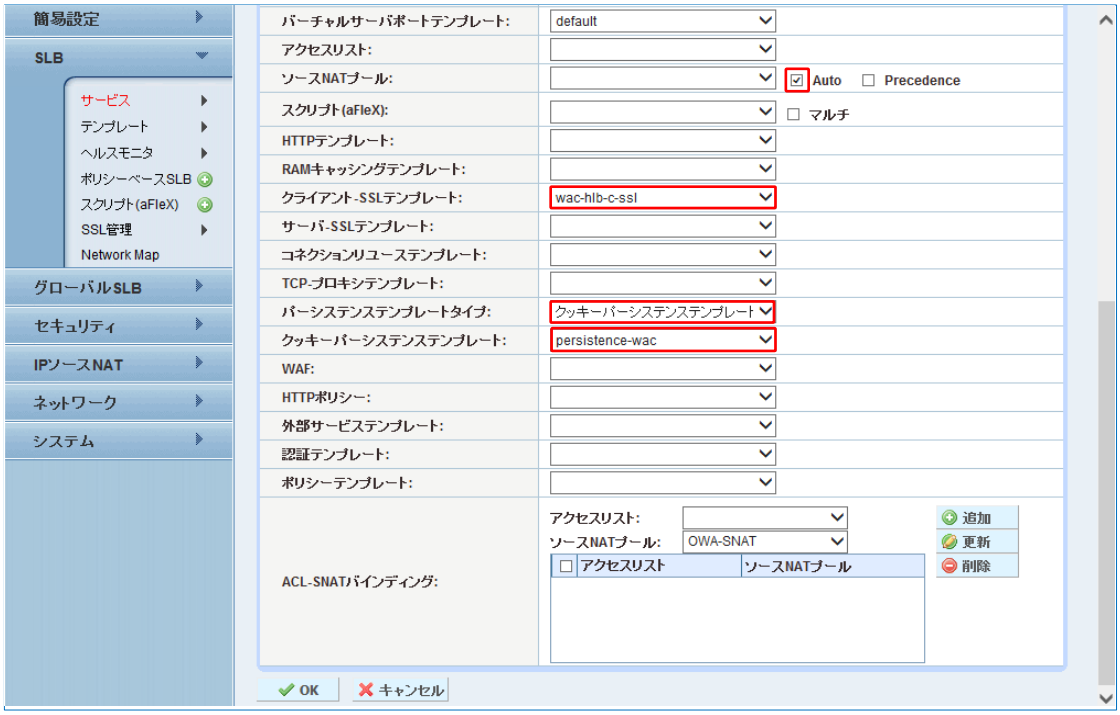

図49：Office Web Appsバーチャルサービスの機能テンプレートの構成

4. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。

7.4 Office Web Apps 向けヘルスモニタ設定

Office Web Apps のヘルスモニタの構成方法を説明します。Office Web Apps サーバーは、”/hosting/discovery” URL への正しいリクエストが来た場合に”wopi-discovery”を返すことを利用し、ヘルスモニタを以下のように構成します。

[コンフィグ] > **[SLB]** > **[ヘルスモニタ]** > **[ヘルスモニタ]**に移動します。

1.
2. **[追加]**ボタンをクリックします。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**WAC-80**
   b. [間隔]：**30**
   c. [タイムアウト]：**10**
   d. [クラス]：**HTTP**
   e. [ポート]： **80**
   f. [URL] ： **GET /hosting/discovery**
   g. [エクスペクト]：**wopi-discovery (テキスト)**

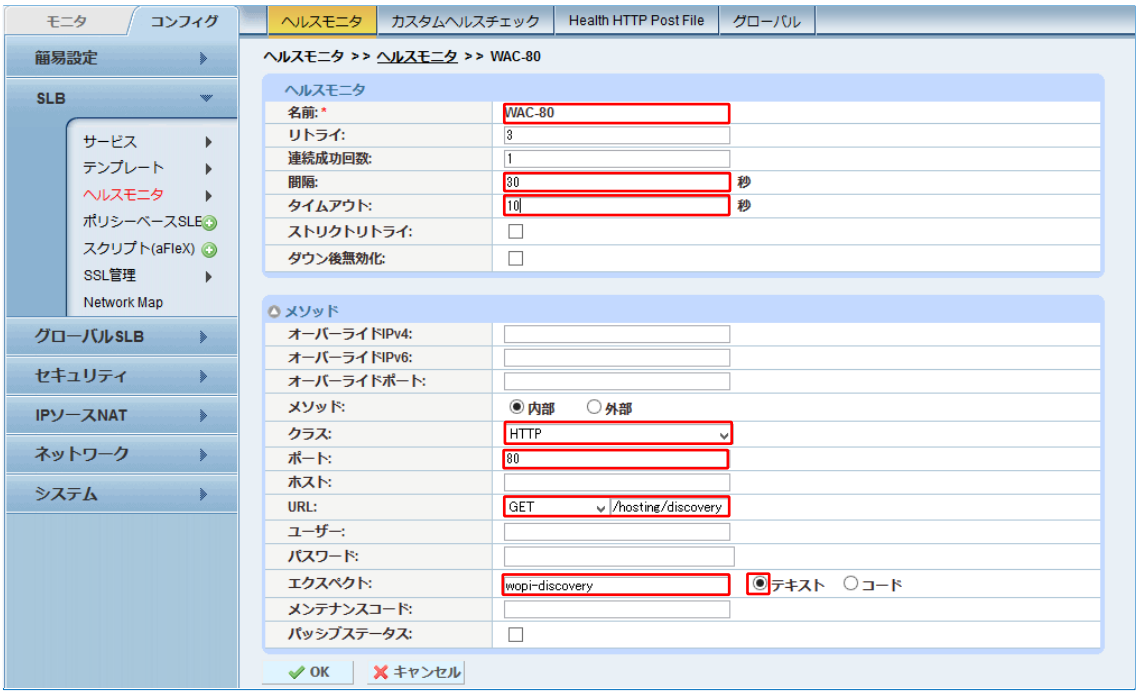

図 50 : Office Web Apps ヘルスモニタの構成

注 : 間隔、タイムアウトについてはユーザ環境におけるサービスレベル等に依存しますので、IT 管理者等適切な方にお問い合わせください。

4. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

7.5 Office Web Apps 向け SSL テンプレート設定

Office Web Apps の SSL オフロード設定時に利用したクライアント SSL テンプレートと証明書の構成を説明します。

最初に、SSL サーバー証明書のインポートを実施します。

1. **[コンフィグ]** > **[SLB]** > **[SSL 管理]** > **[証明書]**に移動します。
2. **[インポート]**ボタンをクリックします。
3. 本構成では、以下の手順で内部証明機関(CA)で発行した Office Web Apps 向け SSL サーバー証明書をインポートします。
   a. [名前]：**wac-hlb.a10domain.a10.com**
   b. [Import Certificate From]：**ローカル**
   c. [Certificate Format] : **PFX**
   d. [パスワード] : 証明書と一緒にファイル化されている秘密鍵のパスワード
   e. [証明書 送信元] : Office Web Apps 向け SSL サーバー証明書のファイルを指定

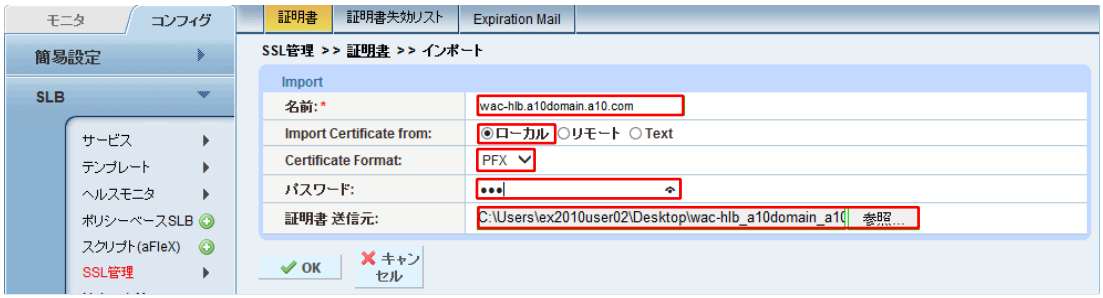

図 51 : Office Web Apps SSL サーバー証明書の構成

注：本構成では、内部証明機関(CA)で発行した SSL サーバー証明書を利用していますが、パブリック証明機関(ベリサイン、DigiCert 等)で発行した SSL サーバー証明書を利用することも可能です。

4. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

証明書のインポート後、クライアント SSL テンプレートを作成します。

5. **[コンフィグ]** > **[SLB]** > **[テンプレート]** > **[SSL]** > **[クライアント SSL]**に移動します。
6. **[追加]**ボタンをクリックします。
7. 本構成では、以下の手順で先ほどインポートした SSL サーバー証明書を利用してクライアント SSL テンプレートを作成します。
   a. [名前]：**wac-hlb-c-ssl**
   b. [証明書名]：**wac-hlb.a10domain.a10.com**
   c. [キー名] : **wac-hlb.a10domain.a10.com**
      << 秘密鍵が証明書ファイルと独立している場合には異なる名前となります。
   d. [パスワード] : 証明書と一緒にファイル化されている秘密鍵のパスワード

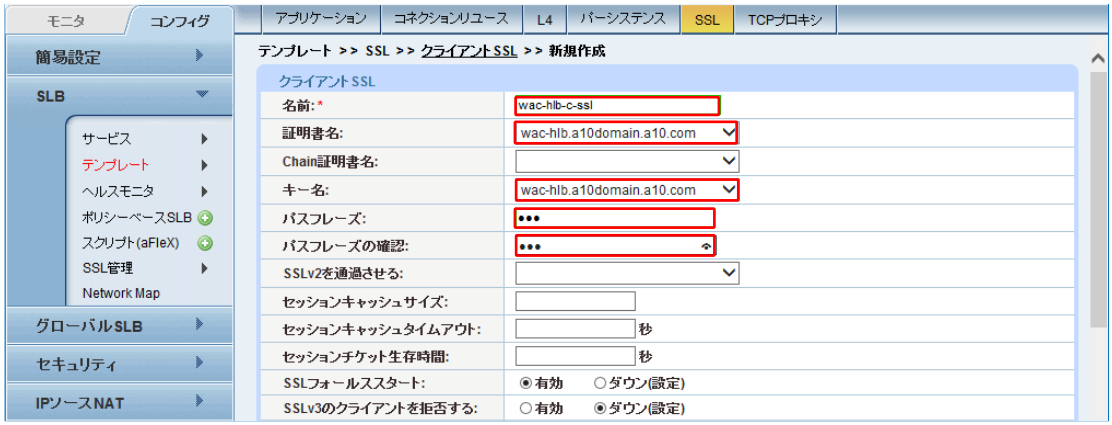

図 52 : Office Web Apps クライアント SSL テンプレートの構成

8. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

7.6 Office Web Apps 向けクッキーパーシステンステンプレート設定

1. **[コンフィグ]** > **[SLB]** > **[テンプレート]** > **[パーシステンス]** > **[クッキーパーシステンス]** に移動します。
2. **[追加]**ボタンをクリックします。
3. 本構成では、以下の手順でクッキーパーシステンステンプレートを設定します。
   a. [名前]：**persistence-wac**
   b. [マッチタイプ]：**ポート (デフォルト設定)**

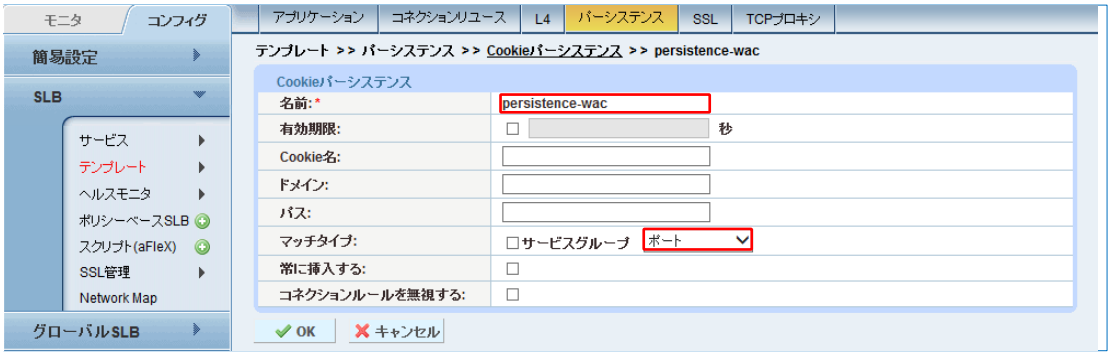

図 53 : Office Web Apps クッキーパーシステンステンプレートの構成

4. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

8 リバースプロキシ

AX/Thunder で、Lync Sever 2013、Office Web Apps サーバー向けにリバースプロキシを構成する方法を記します。リバースプロキシは、両サーバー群が内部ネットワークの Lync クライアントに提供している各種 Web ベースのサービスを外部ネットワーク(インターネット)に公開するために利用されます。

AX/Thunder でリバースプロキシを構成する方法の詳細については、下記リンクのドキュメントを参照願います。

http://www.a10networks.co.jp/support/files/Lync_RP_Deployment_Guide_v1.pdf

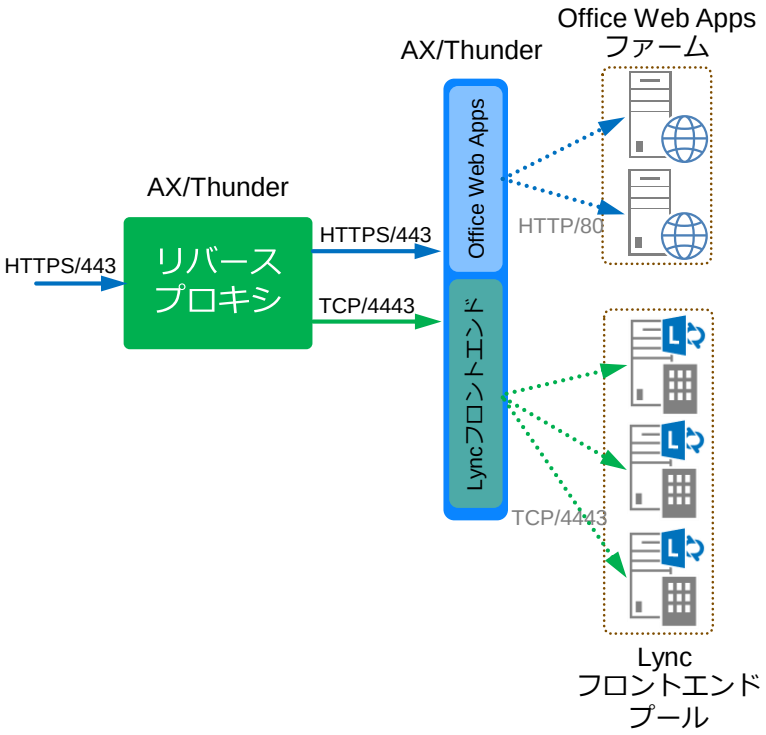

図 54：リバースプロキシの負荷分散構成

8.1　リバースプロキシ用各種証明書のインポート

リモートクライアントからのアクセス要求に対応するための公開用 SSL サーバー証明書と、内部の Lync フロントエンドプールと Office Web Apps ファーム向けに SSL サーバー証明書を発行した内部証明機関(CA)のルート証明書を各々インポートします。

1. **[コンフィグ]** > **[SLB]** > **[SSL 管理]** > **[証明書]**に移動します。
2. **[インポート]**ボタンをクリックします。
3. 本構成では、以下の手順でパブリック証明機関(CA)で発行した Lync Server 2013、Office Web Apps 公開 Web サービス向け SSL サーバー証明書をインポートします。
   a. [名前]：**RP_external**
   b. [Import Certificate From]：**ローカル**
   c. [Certificate Format] : **PFX**
   d. [パスワード] : 証明書と一緒にファイル化されている秘密鍵のパスワード
   e. [証明書 送信元] : Lync Server 2013、Office Web Apps サーバー向け公開用 SSL サーバー証明書のファイルを指定

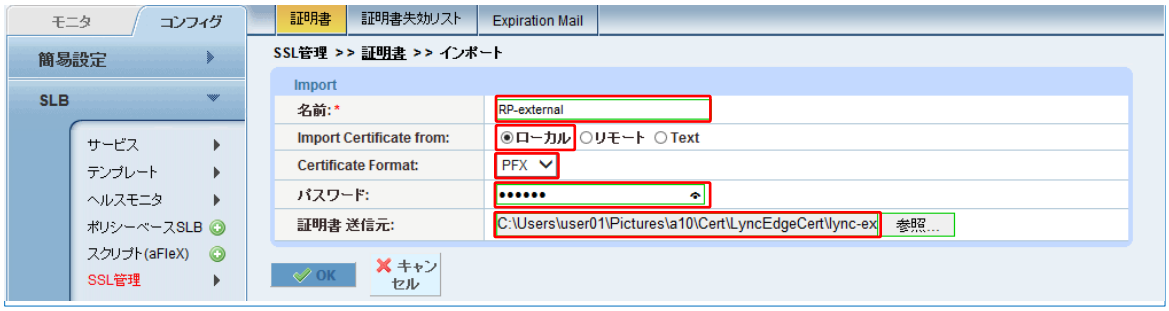

図55：リバースプロキシ公開証明書のインポート

4. **[OK]**ボタンをクリックし、設定を完了します。

続いて、Lync フロントエンドプールと Office Web Apps ファーム向けに SSL サーバー証明書を発行した内部証明機関(CA)のルート証明書をインポートします。

5. 再度**[インポート]**ボタンをクリックします。
6. 本構成では、以下の手順で内部証明機関(CA)のルート証明書をインポートします。
   f. [名前]：**a10domain_a10_local_rootCA**
   g. [Import Certificate From]：**ローカル**
   h. [Certificate Format] : **DER (ルート証明書のファイル形式を選択)**
   i. [証明書 送信元] : 社内認証局のルート証明書ファイルを指定

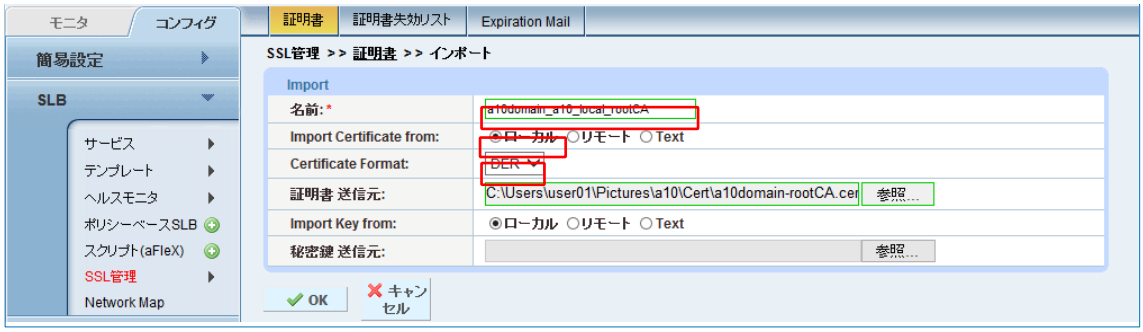

図56 : リバースプロキシ内部ルート証明書のインポート

7. **[OK]**ボタンをクリックし、設定を完了します。

8.2　リバースプロキシ用 SSL テンプレートの設定

先ほどインポートした証明書を利用し、クライアント SSL テンプレートとサーバーSSL テンプレートを作成します。Office Web Apps サーバーのオフロード時には利用しなかったサーバー SSL テンプレートは、外部、内部の 2 つの SSL セッションをブリッジするリバースプロキシの構成では必要となります。

1. **[コンフィグ]** > **[SLB]** > **[テンプレート]** > **[SSL]** > **[クライアント SSL]**に移動します。
2. **[追加]**ボタンをクリックします。
3. 本構成では、以下の手順で先ほどインポートした SSL 証明書でクライアント SSL テンプレートを作成します。
   a. [名前]：**RP-Client-SSL**
   b. [証明書名]：**RP-External**
   c. [キー名] : **RP-External** << 秘密鍵が証明書ファイルと独立している場合には異なる名前となります。
   d. [パスワード] : 証明書と一緒にファイル化されている秘密鍵のパスワード

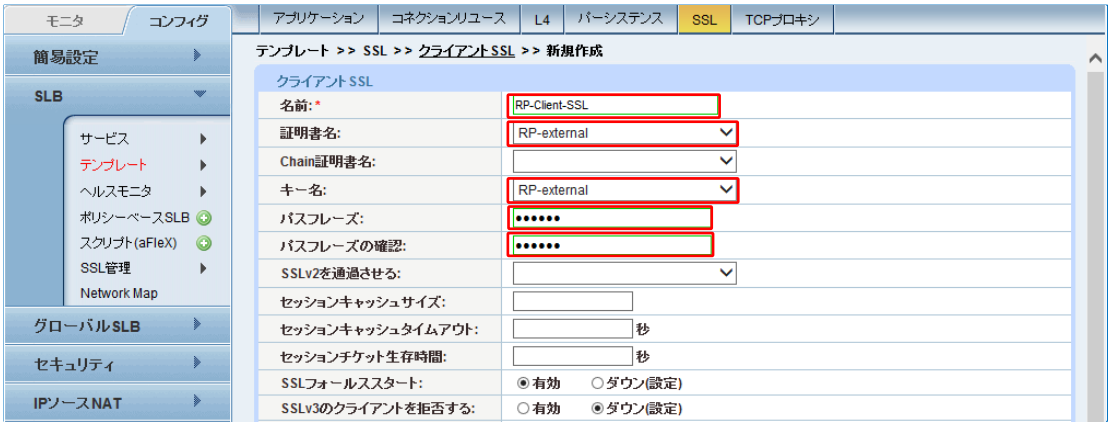

図57：リバースプロキシクライアントSSLテンプレートの構成

4. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

5. **[コンフィグ]** > **[SLB]** > **[テンプレート]** > **[SSL]** > **[サーバーSSL]**に移動します。
6. **[追加]**ボタンをクリックします。
7. 以下の手順で、先ほどインポートした SSL 証明書でサーバーSSL テンプレートを作成します。
   a. [名前]：**RP-Server-SSL**
   b. [CA 証明書] ：先ほどインポートした内部認証局のルート証明書を選択し、**[追加]** ボタンで追加します。

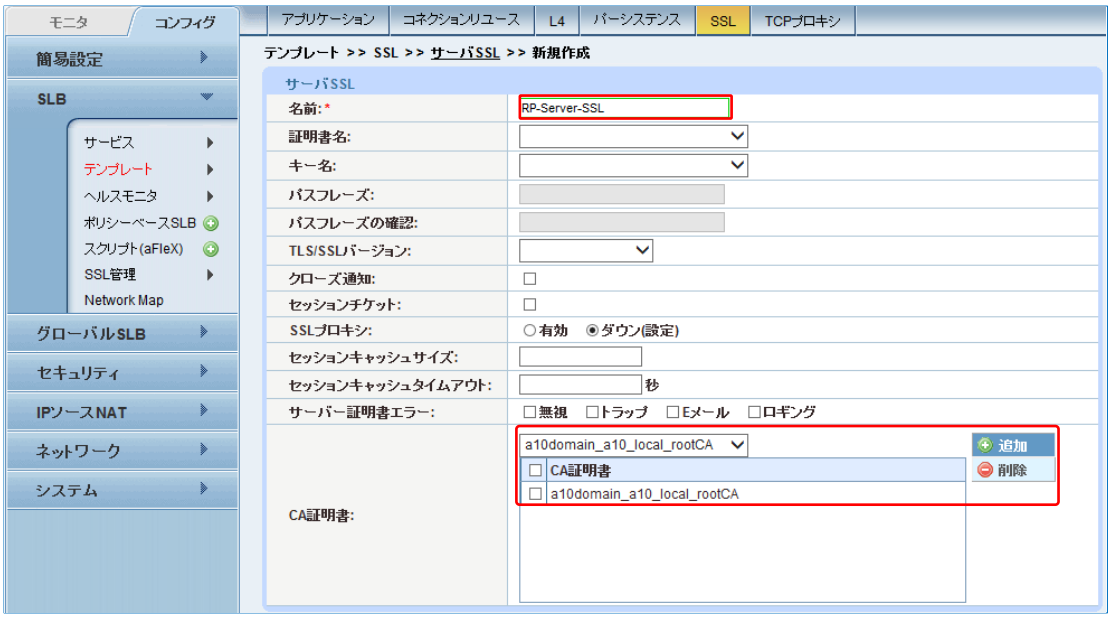

図58：リバースプロキシサーバーSSLテンプレートの構成

8. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

8.3 リバースプロキシ公開サーバーの設定

リバースプロキシでインターネット側に公開する Lync フロントエンドプールと Office Web Apps ファームのサーバーを、Lync フロントエンドプールのロードバランス並びに Office Web Apps ファームのロードバランスで設定した VIP で構成します。

1. **[コンフィグ]** > **[SLB]** > **[サービス]** > **[サーバー]**に移動します。
2. **[追加]**をクリックし、Lync フロントエンドプールで定義した VIP で新しいサーバーを作成します。
3. サーバー設定で、以下の情報を入力します。
   a. [名前]：**Lync-Internal-VIP**
   b. [IP アドレス/ホスト]：**192.168.10.82**
   c. [ヘルスモニタ] : 空白 (ヘルスモニタはサービスグループで設定します)

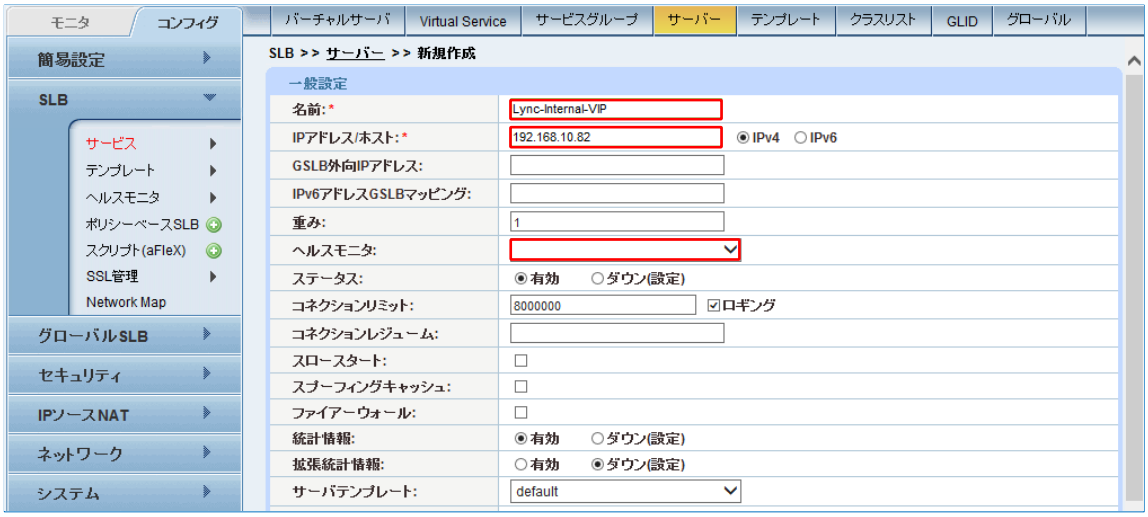

図59：リバースプロキシ サーバーの構成(Lyncフロントエンドプール)

4. **[ポート]**セクションにある**[追加]**を選択し、サーバー構成にポートを追加します。

   a. ポート 4443 を入力、プロトコルタイプで TCP を選択し、ヘルスモニタを空白として、**[追加]**をクリックします。

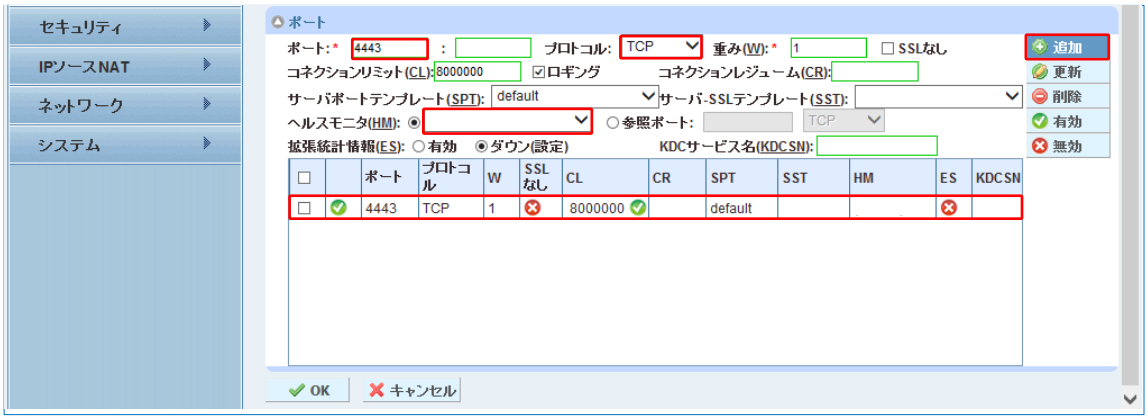

図 60：リバースプロキシ サーバーポートの構成(Lync フロントエンドプール)

5. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

6. 再度**[追加]**をクリックし、Office Web Apps プールで定義した VIP でう新しいサーバーを作成します。
7. サーバー設定で、以下の情報を入力します。
   a. [名前]：**OWA-Internal-VIP**
   b. [IP アドレス/ホスト]：**192.168.10.86**
   c. [ヘルスモニタ] : **空白** (ヘルスモニタはサービスグループで設定します)

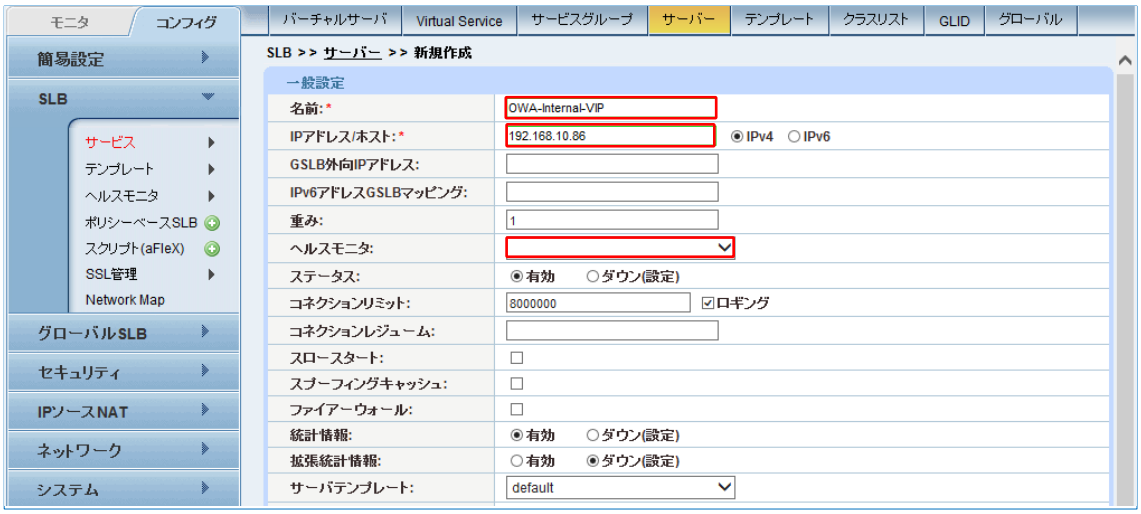

図 61：リバースプロキシ サーバーの構成(Office Web Apps ファーム)

8. **[ポート]**セクションにある**[追加]**を選択し、サーバー構成にポートを追加します。

   a. ポート 443 を入力、プロトコルタイプで TCP を選択し、ヘルスモニタを空白にして、**[追加]**をクリックします。

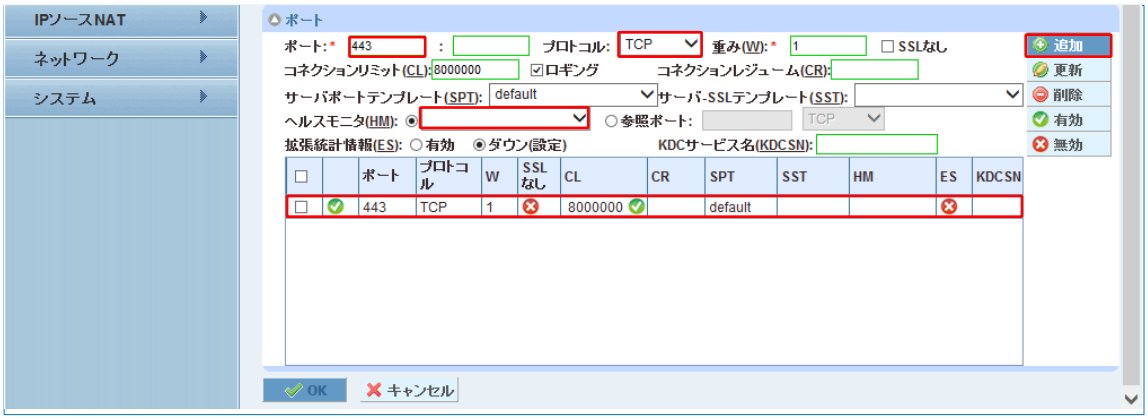

図 62：リバースプロキシ サーバーポートの構成(Office Web Apps ファーム)

9. **[OK]**をクリックした後、**[保存]**をクリックして設定を保存します。

図 63：リバースプロキシサーバーの一覧

8.4 リバースプロキシ用サービスグループの設定

次にリバースプロキシ向けのサービスグループを定義します。

1. **[コンフィグ] >[SLB] > [サービス] > [サービスグループ]**を選択します。
2. **[追加]**をクリックし、「**Lync-443**」という Lync フロントエンドプール用の新しいサービスグループを追加します。
3. 本構成では、以下の情報を設定しています。
   a. [名前]：**Lync-4443**
   b. [クラス]：**TCP**
   c. [アルゴリズム]：**Least Connection**
   d. [ヘルスモニタ]：**HM**

図 64：リバースプロキシサービスグループの構成(Lync フロントエンド)

注：サービスグループは、リアルサーバーとサービスポートのセットで構成され、サーバーの選択アルゴリズムを定義します。

4. **[サーバー]**ドロップダウンリストで**「Lync-Internal-VIP」**を選択し、ポート **4443** で設定します。

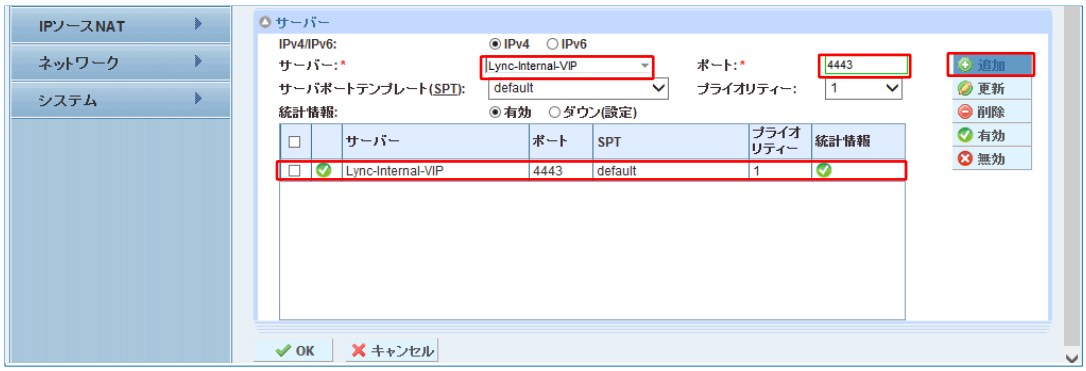

図 65：リバースプロキシサービスグループポートの構成(Lync フロントエンド)

5. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。
6. 1-4 項の設定繰り返し、Office Web Apps ファーム向けに下記設定を実施します。
   a. [名前]：**OWA-443**
   b. [クラス]：**TCP**
   c. [アルゴリズム]：**Least Connection**
   d. [ヘルスモニタ]：**HM**
   e. [ポート] ： **443**

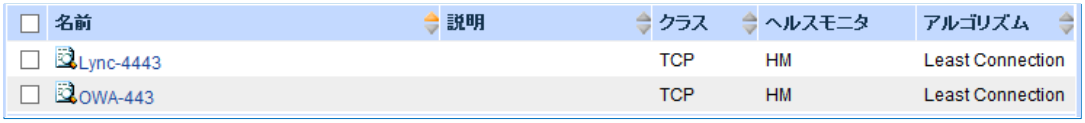

図 66：リバースプロキシサービスグループの一覧

8.5 リバースプロキシ用バーチャルサービスの設定

リバースプロキシのバーチャルサーバーは、バーチャルサービスの設定の一環で構成します。

1. **[コンフィグ]** > **[SLB]** > **[サービス]** > **[バーチャルサーバーポート]**に移動します。
2. **[追加]**ボタンをクリックします。
3. 本構成では、以下の情報を設定しています。
   a. [バーチャルサービス] : **Lync 2013**
   b. [タイプ] : **HTTPS**
   c. [ポート] : **443**
   d. [アドレス] : **172.17.0.108**
   e. [サービスグループ] : **Lync-4443**

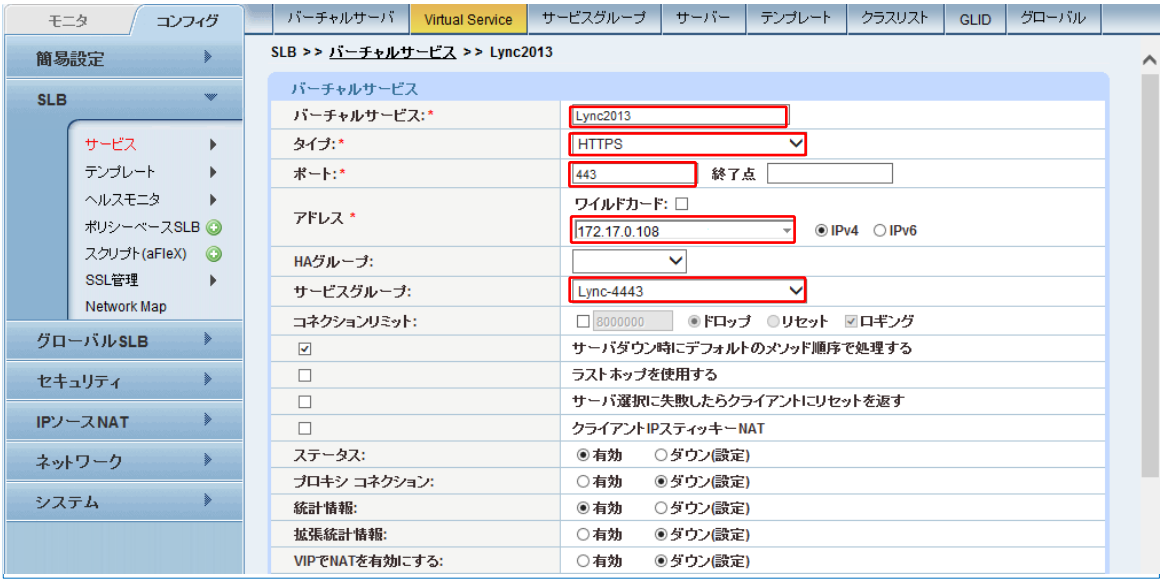

図67：リバースプロキシバーチャルサーバーポートの構成(Lyncフロントエンド)

機能テンプレートとして以下を設定します。

f. [ソース NAT プール]：**Auto**

g. [スクリプト(aFlex)] : **Lync-WAC-Selection** (設定内容については後述)

h. [クライアント SSL テンプレート] : **RP-Client-SSL**

i. [サーバーSSL テンプレート] : **RP-Server-SSL**

j. [パーシステンステンプレートタイプ] ： **クッキーパーシステンステンプレート**

k. [クッキーパーシステンステンプレート： **Cookie-RP**

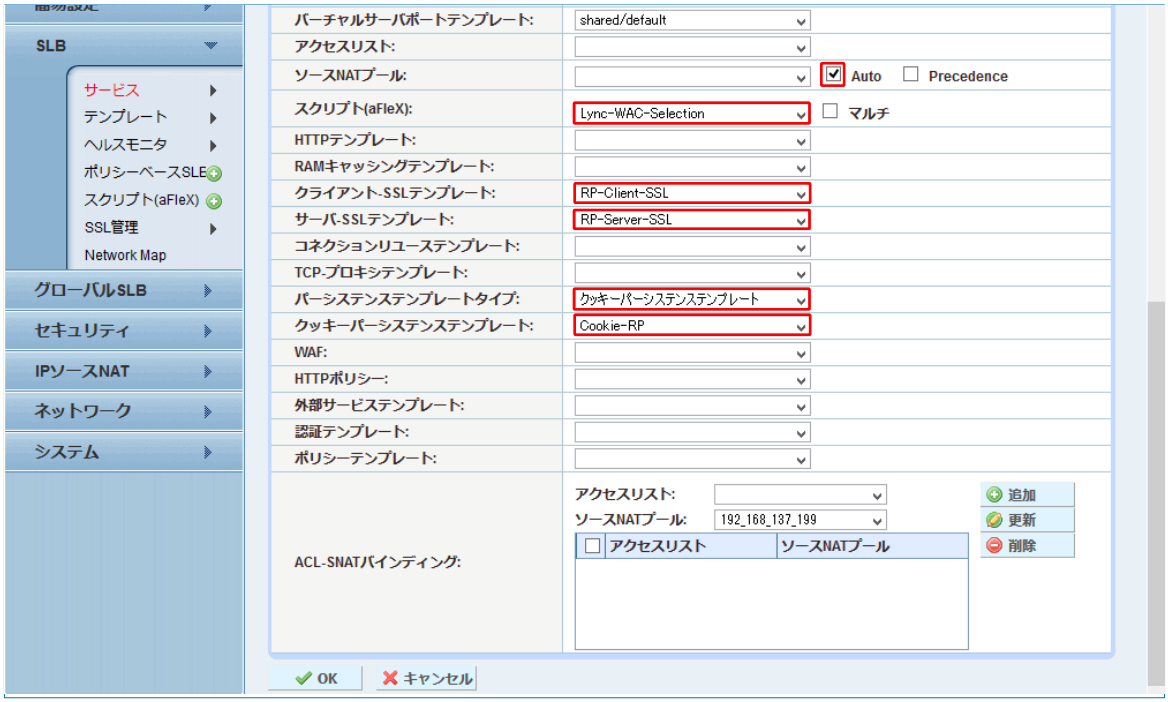

図68：リバースプロキシバーチャルサービス機能テンプレートの構成(Lyncフロントエンド)

注 ： LyncフロントエンドとOffice Web Appsの公開VIPを同じIPアドレスで構成するため、aFleXを活用したFQDN、URL名ベースでの通信の配信を本構成では実施しています。

4. **[OK]**をクリックし、**[保存]**をクリックして構成を保存します。

8.6　リバースプロキシ向け aFleX スクリプト

今回のケースで利用した、FQDN、URL ベースでクライアントからの通信を配信する aFleX スクリプトを以下のように構成しています。同様の処理は HTTP テンプレートでも構成することができます。

1. **[コンフィグ]** > **[SLB]** > **[スクリプト(aFlex)]** に移動します。
2. [追加]ボタンをクリックします。
3. wac-hlb.a10domain.a10.com 以外への通信に関しては、Lync Server 2013 向けサービスグループ Lync-4443 へ配信するルールを以下のように定義しています。
   a. [名前]：**Lync-WAC-Selection**
   b. [定義]：以下の内容を記述

```
when HTTP_REQUEST {
set FQDN [string tolower [HTTP::host]]
switch $FQDN {
   lync2013.a10domain.a10.com {pool Lync-4443}
  dialin.a10domain.a10.com {pool Lync-4443}
  meet.a10domain.a10.com {pool Lync-4443}
  lyncdiscover.a10domain.a10.com {pool Lync-4443}
  wac-hlb.a10domain.a10.com {
     pool OWA-443
  }
}
}
```

注：同スクリプトを定義し、バーチャルサービスで指定することにより、外部公開に必要なグローバル IP アドレスの必要数を最少化することができます。

9 動作確認

正常時、障害時(サーバーダウン、ネットワークダウン)、以下の項目について確認テストを実施し、AX/Thunder が Lync システムの負荷分散装置、リバースプロキシとして正常に動作することを確認しております。

端末種別	大項目	小項目
Lync 2013 (内部ネットワーク/ 外部ネットワーク)	基本	サインイン
		アドレス帳
		プレゼンス変更（手動）
	インスタントメッセージ	二者間インスタントメッセージ
		三者間インスタントメッセージ
		ファイル転送
	音声機能	二者間通話
		三者間音声会議
	ビデオ機能	二者間ビデオ通話
	共有機能	デスクトップ共有
		アプリケーション共有
		パワーポイント共有
		ホワイトボード
	Outlook 連携	不在着信履歴
		会話履歴
Lync Web App (外部ネットワーク)	基本	サインイン
	インスタントメッセージ	二者間インスタントメッセージ
		三者間インスタントメッセージ
		ファイルのアップロード/ダウンロード
	音声機能	二者間通話
		三者間音声会議
	ビデオ機能	二者間ビデオ通話
	共有機能	デスクトップ共有
		アプリケーション共有
		パワーポイント共有
		ホワイトボード
Lync Mobile for iPhone (外部ネットワーク)	基本	サインイン
		表示確認
		手動変更
	アドレス帳	ユーザー検索
		グループ表示
	IM	二者間インスタントメッセージ
		三者間インスタントメッセージ
	音声機能	二者間通話
Lync Mobile for iPad (外部ネットワーク)	資料共有	デスクトップ共有
		アプリケーション共有
		パワーポイント共有

10 要約と結論

上記の構成手順では、Microsoft Lync 2013 Server をサポートするための AX/Thunder のセットアップについて説明しています。AX/Thunder を使用して Lync アプリケーションサービスのロードバランシングを実行する場合の主要なメリットは、以下のとおりです。

- トランスペアレントなアプリケーションの負荷共有。
- ユーザのアプリケーションへのアクセス方法に直接的な影響を与えないように、Lync Server 2013 の障害発生時に高い可用性を実現。
- AX/Thunder が透過的に複数の Lync Server に負荷分散を実行することにより、高い処理効率を実現。
- AX/Thunder で SSL 処理を代行することにより、高い接続スループットおよび迅速なエンドユーザのへの応答を実現。
- Microsoft 社 ForeFront TMG 2010 の代わりに、リバースプロキシ機能を提供。
- 標準機能のパーティショニング(ADP)を有効活用することで、複数の役割やサービス向けの負荷分散やリバースプロキシを集約化

AX/Thunder の Advanced Traffic Manager を使用することにより、Microsoft Lync サーバーのすべてのユーザが有意義なメリットを得ることができます。AX/Thunder シリーズ製品の詳細については、以下の URL をご参照してください。

http://a10networks.com/products/axseries.php

http://a10networks.com/resources/solutionsheets.php

http://a10networks.com/resources/casestudies.php

APPENDIX

以下に、実際にテスト時に設定したシステム構成を記します。

- Lync フロントエンド

```
active-partition P4
vlan 510
 untagged ethernet 5 to 6
 router-interface ve 510
!

interface ve 510
 ip address 192.168.10.85 255.255.255.0
!

ip route 0.0.0.0 /0 192.168.10.88
!

health monitor HM
!

health monitor WAC-80 interval 30 timeout 10
 method http url GET /hosting/discovery expect wopi-discovery
!

health monitor "SIP 5060" interval 15
 method sip tcp expect-response-code 448
!

slb server Lync2013FE1 192.168.10.17
   port 135  tcp
   port 443  tcp
   port 444  tcp
   port 4443  tcp
   port 5061  tcp
   port 5065  tcp
   port 5070  tcp
   port 5071  tcp
   port 5072  tcp
   port 5073  tcp
   port 5075  tcp
   port 5076  tcp
 !

slb server Lync2013FE2 192.168.10.18
   disable
   port 135  tcp
   port 443  tcp
   port 444  tcp
   port 4443  tcp
   port 5061  tcp
   port 5065  tcp
```

```
   port 5070  tcp
   port 5071  tcp
   port 5072  tcp
   port 5073  tcp
   port 5075  tcp
   port 5076  tcp
!

slb server Lync2013FE3 192.168.10.19
   disable
   port 135  tcp
   port 443  tcp
   port 444  tcp
   port 4443  tcp
   port 5061  tcp
   port 5065  tcp
   port 5070  tcp
   port 5071  tcp
   port 5072  tcp
   port 5073  tcp
   port 5075  tcp
   port 5076  tcp
!

slb server WAC1 192.168.10.23
   port 443  tcp
   port 80  tcp
!

slb server WAC2 192.168.10.24
   port 443  tcp
   port 80  tcp
!

slb service-group Lync2013SG-135 tcp
    method least-connection
    health-check HM
    member Lync2013FE2:135
    member Lync2013FE1:135
    member Lync2013FE3:135
!

slb service-group Lync2013SG-443 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:443
    member Lync2013FE2:443
    member Lync2013FE3:443
!

slb service-group Lync2013SG-444 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:444
```

```
    member Lync2013FE2:444
    member Lync2013FE3:444
!

slb service-group Lync2013SG-4443 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:4443
    member Lync2013FE2:4443
    member Lync2013FE3:4443
!

slb service-group Lync2013SG-5061 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5061
    member Lync2013FE2:5061
    member Lync2013FE3:5061
!

slb service-group Lync2013SG-5065 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5065
    member Lync2013FE2:5065
    member Lync2013FE3:5065
!

slb service-group Lync2013SG-5070 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5070
    member Lync2013FE2:5070
    member Lync2013FE3:5070
!

slb service-group Lync2013SG-5071 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5071
    member Lync2013FE2:5071
    member Lync2013FE3:5071
!

slb service-group Lync2013SG-5072 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5072
    member Lync2013FE2:5072
    member Lync2013FE3:5072
!

slb service-group Lync2013SG-5073 tcp
    method least-connection
```

```
    health-check HM
    member Lync2013FE1:5073
    member Lync2013FE2:5073
    member Lync2013FE3:5073
!

slb service-group Lync2013SG-5075 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5075
    member Lync2013FE2:5075
    member Lync2013FE3:5075
!

slb service-group Lync2013SG-5076 tcp
    method least-connection
    health-check HM
    member Lync2013FE1:5076
    member Lync2013FE2:5076
    member Lync2013FE3:5076
!

slb service-group WAC-SG-80 tcp
    health-check WAC-80
    member WAC1:80
    member WAC2:80
!

slb template tcp TCP-Lync
   idle-timeout 1200
!

slb template client-ssl WAC-C-SSL
   cert OfficeWebApps
   key OfficeWebApps pass-phrase encrypted
/+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
!

slb template persist source-ip SIP
!

slb template persist cookie pesistence-wac
!

slb virtual-server Lync2013VIP 192.168.10.82
   port 135  tcp
      source-nat auto
      service-group Lync2013SG-135
      template tcp TCP-Lync
      template persist source-ip SIP
   port 443  tcp
      source-nat auto
      service-group Lync2013SG-443
      template tcp TCP-Lync
```

```
    template persist source-ip SIP
  port 444  tcp
    source-nat auto
    service-group Lync2013SG-444
    template tcp TCP-Lync
    template persist source-ip SIP
  port 4443  tcp
    source-nat auto
    service-group Lync2013SG-4443
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5061  tcp
    source-nat auto
    service-group Lync2013SG-5061
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5065  tcp
    source-nat auto
    service-group Lync2013SG-5065
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5070  tcp
    source-nat auto
    service-group Lync2013SG-5070
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5071  tcp
    source-nat auto
    service-group Lync2013SG-5071
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5072  tcp
    source-nat auto
    service-group Lync2013SG-5072
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5073  tcp
    source-nat auto
    service-group Lync2013SG-5073
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5075  tcp
    source-nat auto
    service-group Lync2013SG-5075
    template tcp TCP-Lync
    template persist source-ip SIP
  port 5076  tcp
    source-nat auto
    service-group Lync2013SG-5076
    template tcp TCP-Lync
    template persist source-ip SIP
!

slb virtual-server OWA_VIP 192.168.10.86
```

```
   port 443  https
      source-nat auto
      service-group WAC-SG-80
      template client-ssl WAC-C-SSL
      template persist cookie persistence-wac
!

enable-management service ssh ethernet 5 to 6 ve 510
enable-management service https ethernet 5 to 6 ve 510
!
end
```

- Lync 内部エッジ

```
active-partition P3
vlan 401
 untagged ethernet 3 to 4
 router-interface ve 401
!

interface ve 401
 ip address 172.19.0.211 255.255.255.0
!

ip route 0.0.0.0 /0 172.19.0.241
!

health monitor HM
!

slb server InternalEdge-1 172.19.0.121
   port 443  tcp
   port 3478  udp
   port 5061  tcp
   port 5062  tcp
!

slb server InternalEdge-2 172.19.0.131
   port 5062  tcp
   port 5061  tcp
   port 3478  udp
   port 443  tcp
!

slb service-group InternalEdge-443 tcp
    method least-connection
    health-check HM
    member InternalEdge-1:443
    member InternalEdge-2:443
!

slb service-group InternalEdge-3478 udp
    method least-connection
    health-check HM
    member InternalEdge-1:3478
    member InternalEdge-2:3478
!

slb service-group InternalEdge-5061 tcp
    method least-connection
```

```
    health-check HM
    member InternalEdge-2:5061
    member InternalEdge-1:5061
!

slb service-group InternalEdge-5062 tcp
    method least-connection
    health-check HM
    member InternalEdge-1:5062
    member InternalEdge-2:5062
!

slb template tcp TCP-Lync
  idle-timeout 1200
!

slb template persist source-ip SIP
!

slb virtual-server _172.19.0.101_vserver 172.19.0.101
  port 443  tcp
     name Internal-443
     source-nat auto
     service-group InternalEdge-443
     template tcp TCP
     template persist source-ip SIP
  port 3478  udp
     name Internal-3478-UDP
     source-nat auto
     service-group InternalEdge-3478
     template persist source-ip SIP
  port 5061  tcp
     name Internal-5061
     source-nat auto
     service-group InternalEdge-5061
     template tcp TCP
     template persist source-ip SIP
  port 5062  tcp
     name Internal-5062
     source-nat auto
     service-group InternalEdge-5062
     template tcp TCP
     template persist source-ip SIP
!

end
```

- Lync 外部エッジ

```
active-partition P2
vlan 201
 untagged ethernet 1 to 2
 router-interface ve 201
!

interface ve 201
 ip address 172.17.0.211 255.255.255.0
!
ip route 0.0.0.0 /0 172.17.0.254
!

health monitor HM
!

slb server ExternalEdge1-access 172.17.0.21
   port 443  tcp
   port 5061  tcp
!

slb server ExternalEdge2-access 172.17.0.31
   port 5061  tcp
   port 443  tcp
!

slb server ExternalEdge1-web 172.17.0.22
   port 443  tcp
!

slb server ExternalEdge2-web 172.17.0.32
   port 443  tcp
!

slb server ExternalEdge1-av 172.17.0.23
   port 3478  udp
   port 443  udp
!

slb server ExternalEdge2-av 172.17.0.33
   port 3478  udp
   port 443  udp
!

slb service-group ExternalEdge-access-443 tcp
    method least-connection
    health-check HM
    member ExternalEdge1-access:443
    member ExternalEdge2-access:443
!
```

```
slb service-group ExternalEdge-access-5061 tcp
    method least-connection
    health-check HM
    member ExternalEdge1-access:5061
    member ExternalEdge2-access:5061
!

slb service-group ExternalEdge-web-443 tcp
    method least-connection
    health-check HM
    member ExternalEdge2-web:443
    member ExternalEdge1-web:443
!

slb service-group ExternalEdge-av-443 tcp
    method least-connection
    health-check HM
    member ExternalEdge1-av:443
    member ExternalEdge2-av:443
!

slb service-group ExternalEdge-av-3478 udp
    method least-connection
    health-check HM
    member ExternalEdge1-av:3478
    member ExternalEdge2-av:3478
!

slb template tcp TCP-Lync
   idle-timeout 1200
!

slb template persist source-ip SIP
!

slb virtual-server _172.17.0.111_vserver 172.17.0.111
   port 443  tcp
      name ExternalEdge-ac443
      source-nat auto
      service-group ExternalEdge-access-443
      template tcp TCP-Lync
      template persist source-ip SIP
   port 5061  tcp
      name ExternalEdge-ac5061
      source-nat auto
      service-group ExternalEdge-access-5061
      template tcp TCP-Lync
      template persist source-ip SIP
!

slb virtual-server _172.17.0.112_vserver 172.17.0.112
```

```
   port 443  tcp
     name ExternalEdge-web443
     source-nat auto
     service-group ExternalEdge-web-443
     template tcp TCP-Lync
     template persist source-ip SIP
!

slb virtual-server _172.17.0.113_vserver 172.17.0.113
   port 443  tcp
     name ExternalEdge-av443
     service-group ExternalEdge-av-443
     template tcp TCP-Lync
     template persist source-ip SIP
   port 3478  udp
     name ExternalEdge-av3478
     service-group ExternalEdge-av-3478
     template persist source-ip SIP
!
end
```

- リバースプロキシ

```
active-partition P1
vlan 202
 untagged ethernet 7
 router-interface ve 202
!

vlan 402
 untagged ethernet 8
 router-interface ve 402
!

interface ve 202
 ip address 172.17.0.201 255.255.255.0
!
interface ve 402
 ip address 172.19.0.201 255.255.255.0
!

ip route 0.0.0.0 /0 172.17.0.254
ip route 192.168.10.0 /24 172.19.0.241
ip route 172.18.0.0 /24 172.19.0.241
!

health monitor HM
!

slb template server-ssl RP-Server-SSL
   ca-cert a10domain_a10_local_rootCA
!

slb server Lync-Internal-VIP 192.168.10.82
   port 4443  tcp
!

slb server OWA-Internal-VIP 192.168.10.86
   port 443  tcp
!

slb service-group Lync-4443 tcp
    method least-connection
    health-check HM
    member Lync-Internal-VIP:4443
!

slb service-group OWA-443 tcp
    method least-connection
```

```
    health-check HM
    member OWA-Internal-VIP:443
!

slb template client-ssl RP-Client-SSL
   cert 20131007RP-2
   key 20131007RP-2 pass-phrase encrypted
/+mboU9rpJM8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
!

slb template persist cookie Cookie-RP
!
!

slb virtual-server _172.17.0.108_vserver 172.17.0.108
   port 443  https
      name Lync2013
      source-nat auto
      service-group Lync-4443
      template client-ssl RP-Client-SSL
      template server-ssl RP-Server-SSL
      template persist cookie Cookie-RP
      aflex Lync-WAC-selection
!

enable-management service https ethernet 7 to 8 ve 202 ve 402
!

end
```