『Cisco Expressway IP ポート使用設定ガイド』（X14.3 および X15.0 リリースを含む）

初版：2024 年 1 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

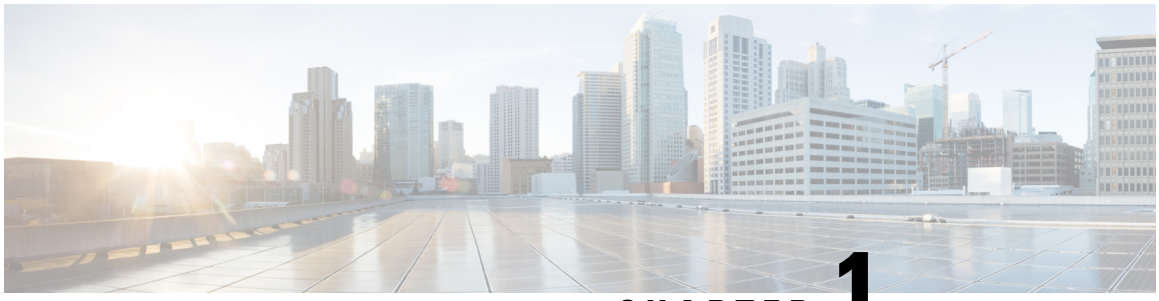
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

このガイドの使用方法

このガイドの目的は、Expressway 展開に関連するインフラストラクチャ コンポーネント間の接続の設定とトラブルシューティングを支援することです。

一般的な Expressway 展開ごとにセクションがあります。それぞれに、主要なインフラストラクチャ コンポーネントとそれらの間の接続を示す図があり、接続も表形式でリストされています。

展開は、必要に応じて相互に構築されます。たとえば、モバイルおよびリモートアクセス（MRA）を実装する場合は、最初にトラバーサルペアを設定します。これらの関係については、関連する導入ガイドで説明されています。

Expressway のコンテキストでのトランスポートとしての TLS（トランスポート層セキュリティ プロトコル）へのガイド内の参照は、TLS が構築されている基盤となる TCP トランスポート プロトコルと同じことを意味します。

この章では、次の内容について説明します。

変更履歴

表 *1 : Cisco Expressway IP* ポートの使用設定ガイドの変更履歴

日付	変更内容	理由
2024 年 1 月	対処済み CDETS：X14.3 および X15.0 の更新を含む	X15.0 リリース
2020 年 5 月	X12.6 用に更新	X12.6 リリース

日付	変更内容	理由
2020 年 4 月	修正	Meeting Server ポートリファレンステーブルの Web プロキシのトンネルメディアのエントリ w をポート 443 から 3478 に修正。また、このガイドのコンテキストでは、トランスポートは TCP と同じであるため、TLS を明記。
2020 年 3 月	修正	欠落している Webbridge シグナリングエントリを Meeting Server ポートリファレンス用の Web プロキシテーブルに追加。
2020 年 2 月	修正	HTTPS/TLS に固定されたヘッドセット設定ファイルの MRA 接続。
2019 年 12 月	更新	[Meeting Server を使用したポイント ツー ポイント Microsoft 相互運用性（Point to Point Microsoft Interoperability Using Meeting Server）] の図に、Meeting Server のロードバランシングがある場合とない場合の両方のメディア パスを示します。
2019 年 7 月	更新	「ヘッドセット管理の MRA 接続」を更新。
2019 年 5 月	更新	NAT リフレクションは、CMS 接続用の Web プロキシには必要ありません（スタンドアロン Expressway の場合のみ）。
2019 年 2 月	更新	Meeting Server の Web プロキシのファイアウォールで NAT リフレクションを設定する方法の詳細を追加。
2019 年 1 月	X12.5 用に更新	X12.5 リリース。ACME 証明書、SIP OAuth、および MRA の ICE パススルー。
2018 年 9 月	更新	X8.11 が使用できなくなったため、ソフトウェアバージョンを X8.11 から X8.11.1 に変更しました。
2018 年 8 月	更生	Cisco Meeting Server 接続の Microsoft クライアントおよび Web プロキシとの IM&P フェデレーションでエラーが発生しました。
2018 年 7 月	X8.11 用に更新。	X8.11 リリース
2018 年 4 月	更生	CMS メディア接続用の SIP Edge で誤記。
2017 年 12 月	更生	SIP トラバーサルコールの場合、Expressway-C の B2BUA は Expressway-E に TURN リクエストを行う必要があります。

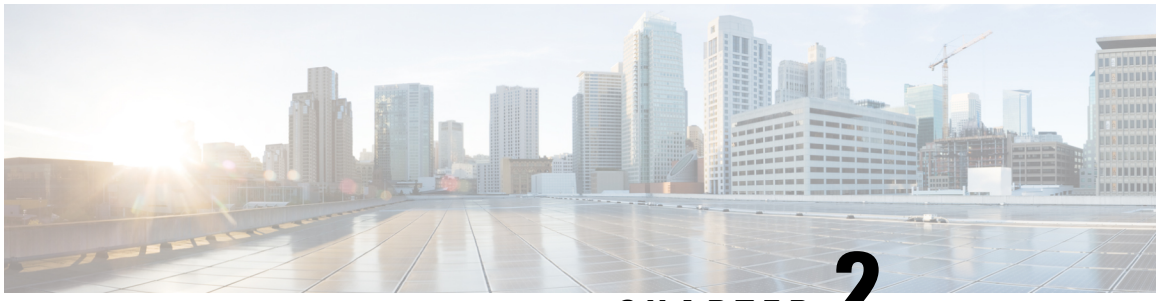
日付	変更内容	理由
2017 年 11 月	更生	Webプロキシメディア接続のエラー。
2017 年 7 月	更新	X8.10 リリース。443 に設定可能な TURN リスニングポート。
2017 年 4 月	新しいドキュメント	以前に「ファイアウォール トラバーサル用の *Expressway IP* ポートの使用状況」に記載されていた情報の新しい形式。

関連資料

表 *2*: 関連ドキュメントとビデオへのリンク

サポートビデオ	Cisco TAC エンジニアから提供される特定の共通の表現の設定手順に関するビデオは、「Expressway/VCS スクリーンキャスト ビデオ リスト」ページにあります。
インストール：仮想マシン	『Expressway 設置およびアップグレードガイド』ページの『*Cisco Expressway* 仮想マシン設置ガイド』
インストール：物理アプライアンス	『Cisco Expressway CE1200 アプライアンス設置ガイド』ページの『*Cisco Expressway CE1200* アプライアンス 設置ガイド』
レジストラ / 単一システムの基本設定	『Expressway 設置ガイド』ページの『*Cisco Expressway* レジストラ導入ガイド』
ファイアウォール トラバーサル / ペアリング対象システムの基本設定	『Expressway 設定ガイド』ページの『*Cisco Expressway-E* および *Expressway-C* 基本設定導入ガイド』
管理およびメンテナンス	「Expressway メンテナンスおよび操作ガイド」ページの『*Cisco Expressway* 管理者ガイド』 「Expressway メンテナンスおよび操作ガイド」ページの『*Cisco Expressway* 有用性ガイド』
クラスタ	「Expressway 設定ガイド」ページの『*Cisco Expressway* クラスタの作成とメンテンナンス導入ガイド』

証明書	「Expressway 設定ガイド」ページの『*Cisco Expressway* 証明書の作成と使用導入ガイド』
MRA	「Expressway 設定ガイド」ページの『*Cisco Expressway* 経由の *Mobile & Remote Access*』
Cisco Meeting Server	「Expressway 設定ガイド」ページの『*Cisco Expressway* での *Cisco Meeting Server* 導入ガイド』 「Cisco Meeting Server プログラミングガイド」ページの『*Cisco Meeting Server API* リファレンスガイド』 その他の Cisco Meeting Server のガイドは、「Cisco Meeting Server 設定ガイド」ページで公開されています。
Cisco Webex ハイブリッドサービス	ハイブリッド サービス ナレッジ ベース
Cisco Hosted Collaboration Solution（HCS）	HCS のお客様用マニュアル
Microsoft インフラストラクチャ	「Expressway 設定ガイド」ページの『*Microsoft* インフラストラクチャ での *Cisco Expressway* 導入ガイド』 「Expressway 設定ガイド」ページの『*Cisco Jabber* およびビジネス版 *Microsoft Skype* インフラストラクチャ設定チートシート』
REST API	「Expressway 設定ガイド」ページの『*Cisco Expressway REST API* サマリーガイド』（API が自己文書化されている高レベル情報のみ）
MultiWay 会議	「Expressway 設定ガイド」ページの『*Cisco TelePresence Multiway* 導入ガイド』



CHAPTER 2

ファイアウォール設定

このドキュメントで説明されている接続を許可するようにファイアウォールを設定する場合は、次の点に注意してください。

- Expressway のクラスタがある場合は、各 Expressway ピアのパブリック IP アドレスへの宛先ポートが外部ファイアウォールで開いていることを確認します。
- 場合によっては、同じタスクを実行するために使用できるさまざまな接続タイプがあります。図と表に示されているすべてのポートを開く必要はありません。使用していないポートを閉じることをお勧めします。

  たとえば、Web 管理ポートが TCP 7443 で、SSH のみを使用して Expressway を設定する場合は、7443 を閉じて TCP 22 を開いたままにすることができます。管理ポートは、ネットワーク内部からの接続に対してのみ開く必要があります。
- 一部のファイアウォールは、非アクティブに見える接続をアクティブに閉じるため、ビデオインフラストラクチャの動作に干渉する可能性があります。

  たとえば、TCP ポート 1720 は H.323 コールシグナリングに使用されますが、コール中は非アクティブである可能性があります。これがファイアウォールによって時期尚早に閉じられた場合、H.323 エンドポイントはそれをドロップされたコールとして解釈し、コールを切断することで応答する可能性があります。

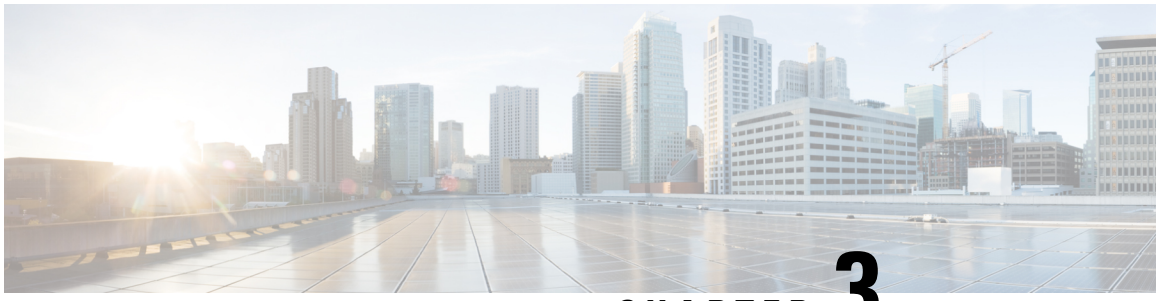
  既知のポートでの非アクティブタイムアウトを少なくとも 2 時間に延長することを推奨します。特に、特定の期間後にコールが失敗する場合はそうです。
- SIP/H.323 プロトコル用の ALG（アプリケーション レイヤ ゲートウェイ）を含むファイアウォールは、Expressway-E で期待どおりに機能しない場合があります。

  NAT ファイアウォールで SIP または H.323 ALG インスペクション/認識を無効にすることを強く推奨します。この変更を行うことができない場合、設定をサポートできない可能性があります。

  メディアの問題を回避するために、NAT ファイアウォールで UDP インスペクションを無効にすることを推奨します。
- 一部の展開では、メディアパケットが Expressway-E の外部 NIC でヘアピンすることがあります。一部のファイアウォールは、ヘアピニングを許可せず、独自の送信元宛てのパケットを信頼しません。

展開で必要な場合は、Expressway-Eパブリックインターフェイスでヘアピニングを許可するように例外を設定することをお勧めします。

- Expressway-E のスタティック NAT 機能を使用する場合は、2 つの NIC を使用することを強く推奨します。1 つの NIC を外部インターフェイス専用にし、もう 1 つを内部インターフェイス専用にする方が、スタティック NAT が有効になっている 1 つの NIC を使用するよりもはるかにネットワークに適しています。



CHAPTER 3

デフォルトのポート範囲

このドキュメントでは、次のデフォルトが使用されています。デフォルトのポート範囲は、新機能の開発に伴い（やむを得ない場合は）変更されることがあります。シスコのドキュメントには、特定のバージョン番号の現在のデフォルトポートがリストされています。

Note このドキュメントでは、サードパーティのインフラストラクチャで使用されるポート範囲を記載している場合があります。これらはデフォルト値であり、ご使用の環境に対して正しいことを保証するものではありません。サプライヤのマニュアルに従って、これらの接続を設定することをお勧めします。

Table 3: Expressway **のデフォルト ポート範囲**

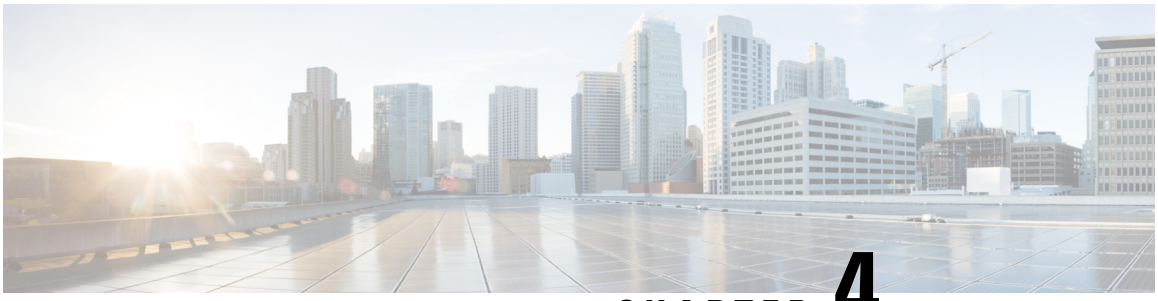
プロトコル	用途	現在の範囲	詳細
TCP	エフェメラルポート	1024 ～ 65535	アウトバウンド HTTP/S、LDAP
UDP	エフェメラルポート	1024 ～ 65535	DNS、アウトバウンド TURN リクエスト
TCP	エフェメラルポート	30000 ～ 35999	
UDP	エフェメラルポート	30000 ～ 35999	
TCP	アウトバウンド SIP	25000 ～ 29999	
UDP&TCP	小規模/中規模 Expressway-E でのインバウンド TURN リクエスト	3478	Expressway-E のみ。443 または 1024 以上の任意のポートに設定可能

プロトコル	用途	現在の範囲	詳細
UDP&TCP	大規模 Expressway-E でのインバウンド TURN リクエスト	3478 ～ 3483	大規模 Expressway-E のみ。最初のポートが 1024 以上の 6 ポート範囲に設定可能。 ポート多重化が有効になっている場合は、単一のポートに設定できます。TURN ポート多重化の詳細については、『Cisco Expressway 管理者ガイド』を参照してください。
TCP	Cisco Expressway-E でのインバウンド TCP TURN リクエスト	443	Expressway-E で、TCP 443 TURN サービスが有効になっている場合のみ。
UDP	TURN リレー	24000 ～ 29999	Expressway-E のみ。
UDP	RTP/RTCP メディア	36000 ～ 59999	範囲は、デフォルトの範囲内で設定できます。たとえば、37000 ～ 38200 ですが、35000 ～ 36200 ではありません。 S/M Expressway では、デフォルト/カスタムポートを使用しない場合、最初の 2 つのポートを多重化メディアに使用できます。 Expressway では、範囲の最初の 12 個のポートが多重化メディアに使用されます。そのサブ範囲をカスタマイズすることはできません。

プロトコル	用途	現在の範囲	詳細
UDP	小規模/中規模 Expressway-E システム上の多重化メディア	2776/2777 または 36000/36001	2776/2777 は古いペアですが、S/M システムオプションで新しいデフォルト範囲が導入されたときにカスタマイズする機能により、デフォルトとして保持されます。カスタムペアは、 **設定** > **トラバーサル**>**ポート** で定義されます。 Expressway-E のみ。 **Note** 接続マップとポート参照では、わかりやすくするためにすべてのポートオプションを示していません。たとえば、図には 2776/2777 と表示されているが、代わりに 36000/36001 を使用することを選択した場合は、2776/2777 も開く必要はありません。

プロトコル	用途	現在の範囲	詳細
UDP	大規模 Expressway-E システムの多重化メディア	36000 ～ 36011	大規模システムオプションで導入された新しい範囲。この範囲は、常に RTP/RTCP メディア範囲の最初の 12 ポートであるため、別のメディア範囲を設定した場合は異なります。 Expressway-E 大規模 OVA または大規模アプライアンスのみ。 **Note** 接続マップとポート参照では、わかりやすくするためにすべてのポートオプションを示していません。たとえば、図に 2776/2777 と表示されているが、Expressway が大きい場合は、2776/2777 ではなく、メディア範囲の最初の 12 個のポートを開く必要があります。

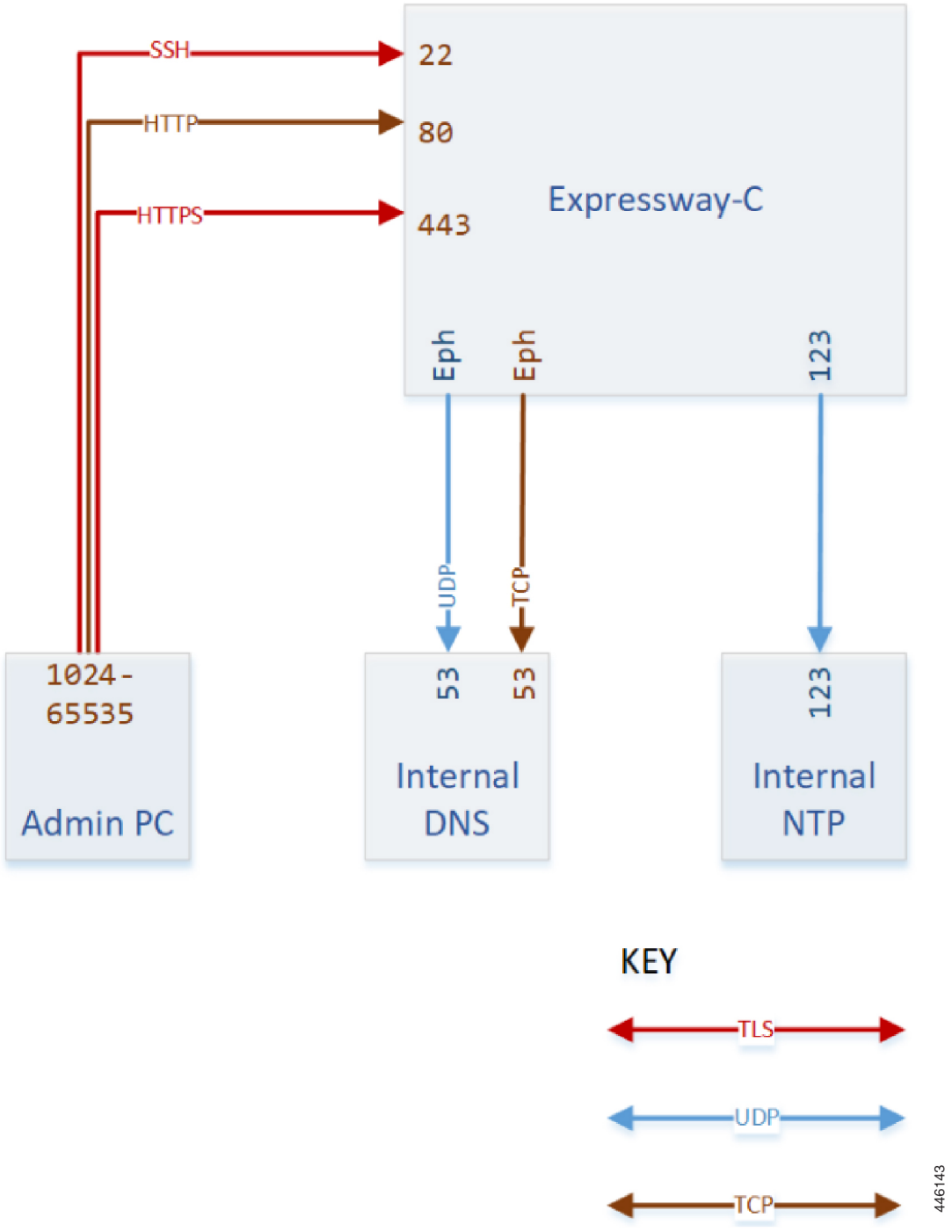
プロトコル	用途	現在の範囲	詳細
TCP	SIP トラバーサル	7001	設定可能。最初の Expressway-E トラバーサル サーバー ゾーンの SIP リスニングポート。後続のトラバーサル サーバー ゾーンは、増分ポート番号を使用します。デフォルトでは 7002 です。
UDP	H.323 トラバーサル	6001	設定可能。最初の Expressway-E トラバーサル サーバー ゾーンの H.323 リスニングポート。後続のトラバーサル サーバー ゾーンは、増分ポート番号を使用します。デフォルトでは 6002 です。



CHAPTER 4

基本的なネットワーキング接続

基本的なネットワーキング：Expressway



ネットワーキング ポート リファレンス：Expressway

表 *4 : Expressway-C* の基本的なネットワーキングポート

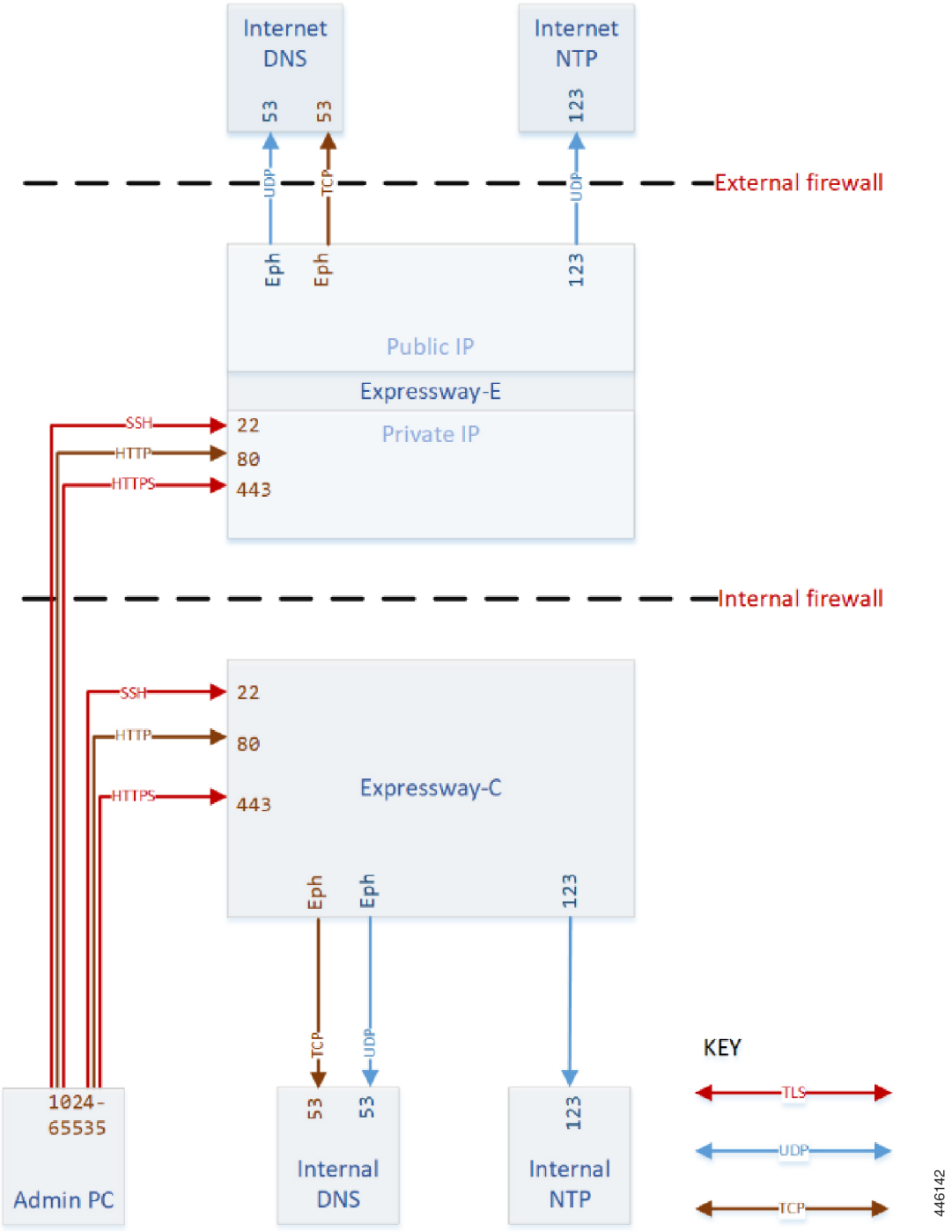
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
管理者 SSH	管理者 PC	1024 ～ 65535	TCP	Expressway-C	22 または 5022[1]
管理者 HTTP*	管理者 PC	1024 ～ 65535	TCP	Expressway-C	80
管理者 HTTPS	管理者 PC	1024 ～ 65535	TCP	Expressway-C	443
名前解決（DNS）	Expressway-C	30000 ～ 35999	UDP & TCP §	内部ネームサーバー	53
同期時刻（NTP）	Expressway-C	123	UDP	内部時間サーバー	123

* Expressway はデフォルトで HTTP を HTTPS にリダイレクトします。HTTP ポートを開く必要はありませんが、便宜上 HTTP を許可し、HTTPS にリダイレクトできます。

§ レスポンスが大きすぎる場合、Expressway は TCP を介して DNS 解決を試みます。

（注） [1]ポート 22 は、Expressway アプライアンスの管理者 SSH ポートとして設定されます。Expressway 仮想マシンは、VM の展開時にポート 22 または 5022 に展開できます。

基本的なネットワーキング：トラバーサルペア



ネットワーキング ポート リファレンス：Expressway トラバーサルペア

表 *5 : Expressway-C* の基本的なネットワーキングポート

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
管理者 SSH	管理者 PC	1024 ～ 65535	TCP		22 または 5022[1]
管理者 HTTP*	管理者 PC	1024 ～ 65535	TCP	Expressway-C	80
管理者 HTTPS	管理者 PC	1024 ～ 65535	TCP	Expressway-C	443
名前解決（DNS）	Expressway-C	30000 ～ 35999	UDP & TCP §	内部ネームサーバー	53
同期時刻（NTP）	Expressway-C	123	UDP	内部時間サーバー	123

* Expressway はデフォルトで HTTP を HTTPS にリダイレクトします。HTTP ポートを開く必要はありませんが、便宜上 HTTP を許可し、HTTPS にリダイレクトできます。

§ レスポンスが大きすぎる場合、Expressway は TCP を介して DNS 解決を試みます。

（注） [1]ポート 22 は、Expressway アプライアンスの管理者 SSH ポートとして設定されます。Expressway 仮想マシンは、VM の展開時にポート 22 または 5022 に展開できます。

表 *6 : Expressway-E* の基本的なネットワーキングポート

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
管理者 SSH	管理者 PC	1024 ～ 65535	TCP	Expressway-E プライベート IP	22 または 5022[1]
管理者 HTTP	管理者 PC	1024 ～ 65535	TCP	Expressway-E プライベート IP	80
管理者 HTTPS	管理者 PC	1024 ～ 65535	TLS	Expressway-E プライベート IP	443

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
内部ネーム解決（DNS）*	Expressway-E プライベート IP	30000 ～ 35999	UDP & TCP	内部ネーム サーバー	53
外部ネーム解決（DNS）	Expressway-E パブリック IP	30000 ～ 35999	UDP & TCP	内部ネーム サーバー	53
内部時間同期（NTP）*	Expressway-E プライベート IP	123	UDP	内部時間サーバー	123
外部時間同期（NTP）	Expressway-E パブリック IP	123	UDP	外部時間サーバー	123

* Expressway-E を外部 DNS および NTP に接続することもできます。両方は必要ありません。

（注） [1]ポート 22 は、Expressway アプライアンスの管理者 SSH ポートとして設定されます。Expressway 仮想マシンは、VM の展開時にポート 22 または 5022 に展開できます。

ネットワーキング ポート リファレンス：スマートライセンス

（注） Expressway にはスマートライセンスサーバーへの接続が必要であり、ポート要件はスマートライセンスの転送設定によって異なります。表に示されているデバイスの詳細を確認します。

表 *7: Expressway-E* からクラウドへの接続

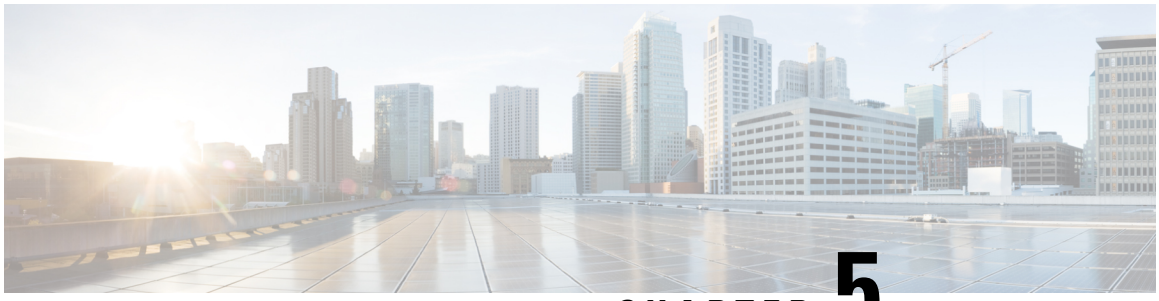
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Expressway-E から発信されるスマート ライセンス リクエスト	Expressway-E	エフェメラル（30000 ～ 35999）	TLS	https://smartreceiver.cisco.com/licservice/license	443
スマート ライセンス ダイレクト	Expressway	1024 ～ 65535	TLS	smartreceiver.cisco.com	443

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
スマート ライセンス オンプレミス CSSM	Expressway	1024 ～ 65535	TLS	ユーザー設定のオンプレミス CSSM IP/FQDN	443
スマートライセンスプロキシ	Expressway	1024 ～ 65535	TLS	ユーザーが設定したプロキシサーバーの IP/FQDN	ユーザー設定のプロキシサーバーポート

ネットワーキングポートリファレンス：電子メール通知サービス

Simple Mail Transfer Protocol（SMTP）サーバーは、暗黙的または明示的な接続用に設定できます。2 つの接続タイプの違いは次のとおりです。

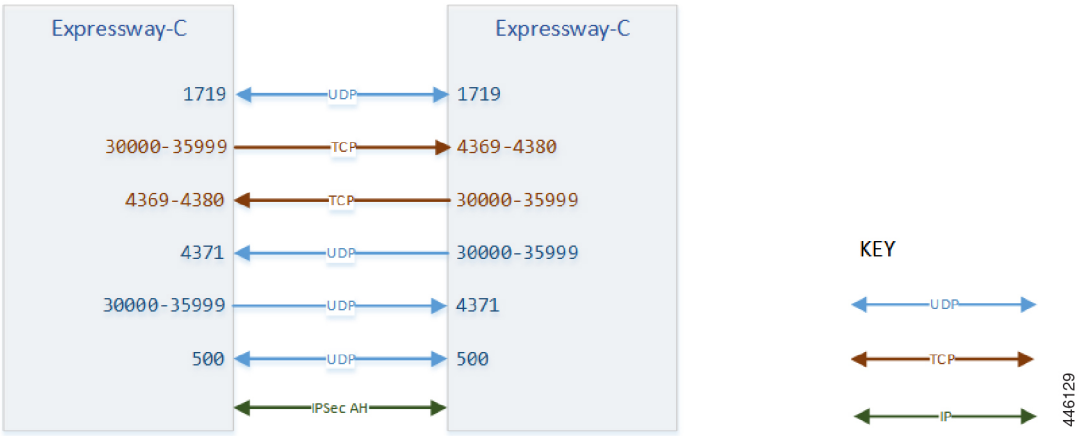
- **明示モード** ：クライアントは最初に SMTP サーバーに接続します。その後、サーバー **は TLS/SSL 暗号化の切り替えを明示的にリクエストします**。デフォルトのポートは25と 587 です。
- **暗黙モード** ：クライアントは SMTP サーバーに接続します。チャネルを確立するとすぐに、サーバーは TLS/SSL 暗号化を **暗黙的**にオンにします。デフォルトの TCP ポートは 465 です。



CHAPTER 5

クラスタ接続

X8.8 より前のクラスタ接続

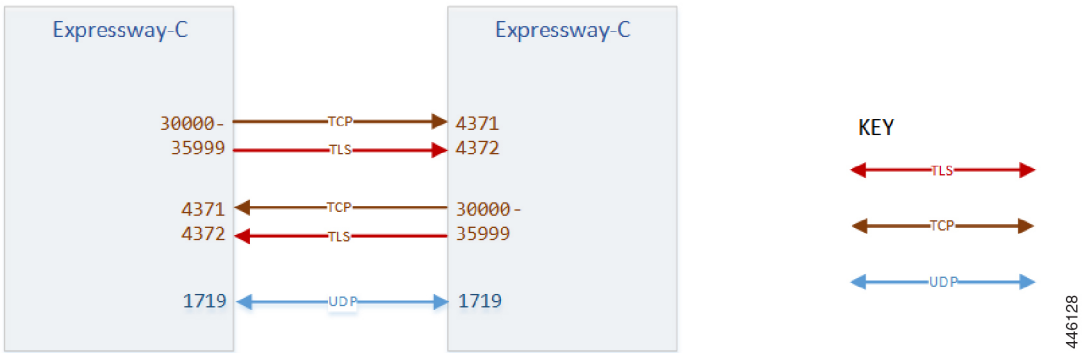


X8.8 より前のクラスタポートリファレンス

表 *8:* クラスタの同期と通信

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
クラスタ データベースの同期（IPSec AH）	このピア	該当なし	51	その他のピア	該当なし
ピア間のキー交換（ISAKMP）	このピア	500	UDP	その他のピア	500
クラスタリカバリ	このピア	30000 ～ 35999	UDP	その他のピア	4371
クラスタ通信	このピア	30000 ～ 35999	TCP	その他のピア	4369 ～ 4380
帯域幅管理（Expressway-C クラスタのみ）	このピア	1719	UDP	その他のピア	1719

クラスタ接続 X8.8 以降



クラスタポートリファレンス X8.8 以降

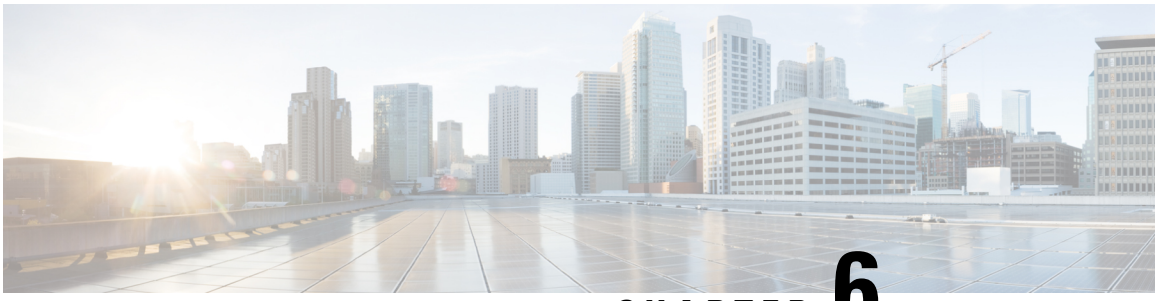
表 *9 : Expressway-C* クラスタデータベースの同期と通信

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
クラスタリカバリ	このピア	30000 ～ 35999	TCP	その他のピア	4371
クラスタ通信	このピア	30000 ～ 35999	TLS	その他のピア	4372
帯域幅管理	このピア	1719	UDP	その他のピア	1719

表 *10 :* ピア間でルーティングされる *SIP* コール（図には表示されていません）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP TCP シグナリング	このピア	25000 ～ 29999	TCP	その他のピア	5061
SIP TLS シグナリング	このピア	25000 ～ 29999	TLS	その他のピア	5061
RTP/RTCP	このピア	36000 ～ 59999	UDP	その他のピア	36000 ～ 59999
帯域幅管理（Bandwidth management）	このピア	1719	UDP	その他のピア	1719

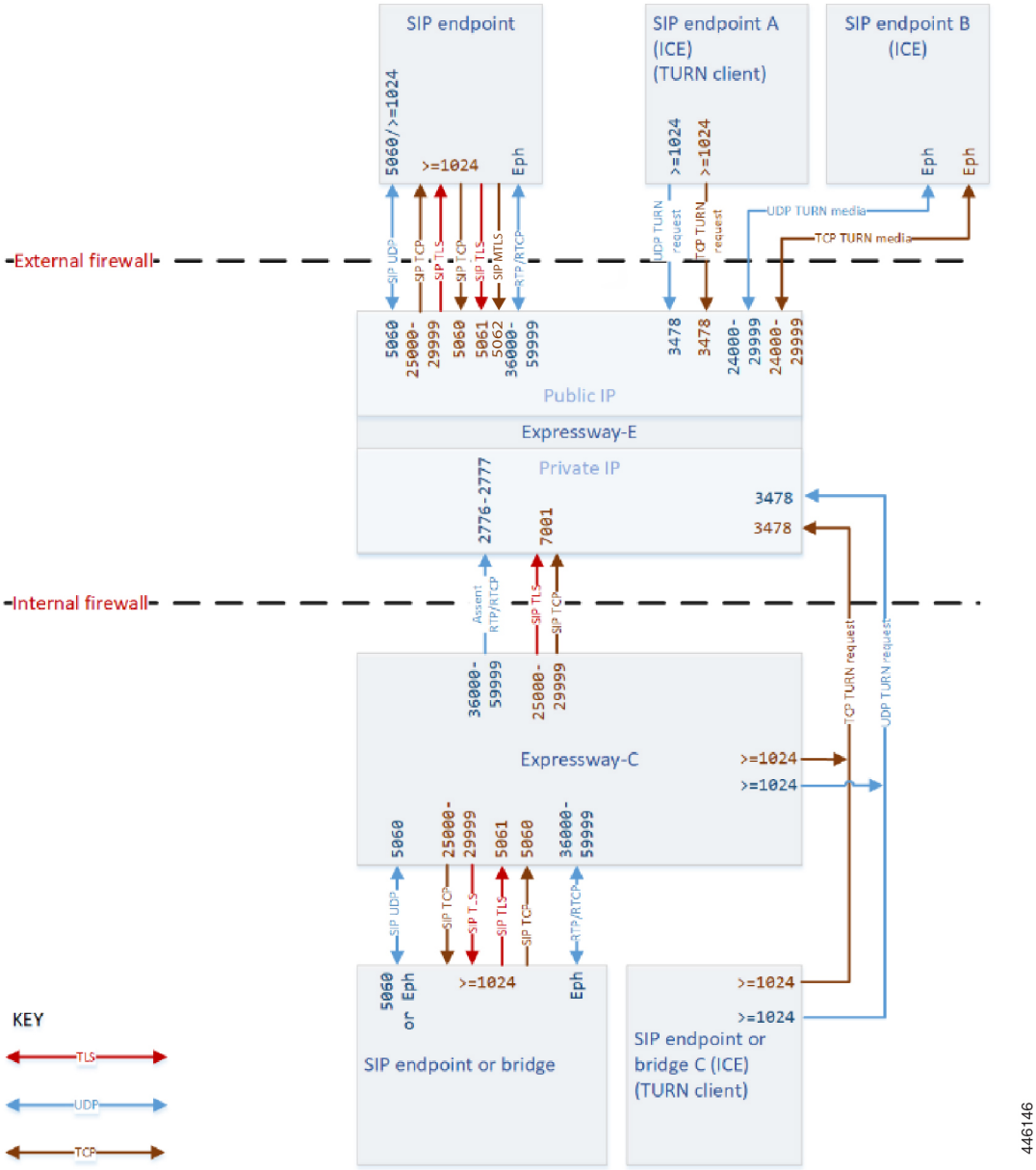
（注） Dbxsh は、ポート 4370 を使用してローカルループバックアドレス上のクラスタ データベースに接続するスクリプトです。Dbxsh は、コマンドを実行する前にデータベースを認証する必要がありません。ポートは接続用に開いており、内部使用のみを目的としています。これはルートからのみアクセスできます。



CHAPTER 6

プロビジョニング登録認証とコール

SIP コール


SIP endpoint
SIP endpoint A (ICE) (TURN client)
SIP endpoint B (ICE)
5060/>=1024
>=1024
Eph
>=1024
>=1024
Eph
Eph
UDP TURN request
TCP TURN request
UDP TURN media
TCP TURN media
External firewall
SIP UDP
SIP TCP
SIP TLS
SIP TCP
SIP TLS
SIP MTLS
RTP/RTCP
5060
25000-29999
5060
5061
5062
36000-59999
3478
3478
24000-29999
24000-29999
Public IP
Expressway-E
Private IP
2776-2777
7001
3478
3478
Internal firewall
Assent RTP/RTCP
SIP TLS
SIP TCP
36000-59999
25000-29999
TCP TURN request
UDP TURN request
Expressway-C
>=1024
>=1024
5060
25000-29999
5061
5060
36000-59999
SIP UDP
SIP TCP
SIP TLS
SIP TLS
SIP TCP
RTP/RTCP
5060 or Eph
>=1024
Eph
>=1024
>=1024
SIP endpoint or bridge
SIP endpoint or bridge C (ICE) (TURN client)
KEY
TLS
UDP
TCP
446146

SIP コールポートリファレンス

表 *11 : SIP* コールポートリファレンス

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP または TLS	Expressway-E	7001（最初のトラバーサルゾーンの場合。2 番目の場合は 7002 など）
SIP シグナリング	Expressway-C	5060	UDP	SIP エンドポイント	5060（多くの場合、異なる場合があります。1024 以上） 登録（登録されている場合）または DNS ルックアップによって定義されたポート番号
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP または TLS	SIP エンドポイント	>=1024 登録（登録されている場合）または DNS ルックアップによって定義されたポート番号
SIP シグナリング	Expressway-E	25000 ～ 29999	TCP または TLS	SIP エンドポイント（またはそのファイアウォール）	>=1024 登録（登録されている場合）または DNS ルックアップによって定義されたポート番号

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	UDP	Expressway-E	[5060] SIP UDP はデフォルトで無効になっています。インターネットに接続する場合は推奨されません。
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	TCP	Expressway-E	[5060] SIP TCP はデフォルトで無効になっています（X8.9.2 以降）。
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	TLS	Expressway-E	5061
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	MTLS	Expressway-E	5062
承認 RTP（トラバースされたメディア）	Expressway-C	36000 ～ 59999	UDP	Expressway-E	2776 または 36000（小規模/中規模） 36000 ～ 36010（偶数ポート）（大規模）
承認 RTCP（トラバースされたメディア）	Expressway-C	36000 ～ 59999	UDP	Expressway-E	2777 または 36001（小規模/中規模） 36001 ～ 36011（奇数ポート）（大規模）

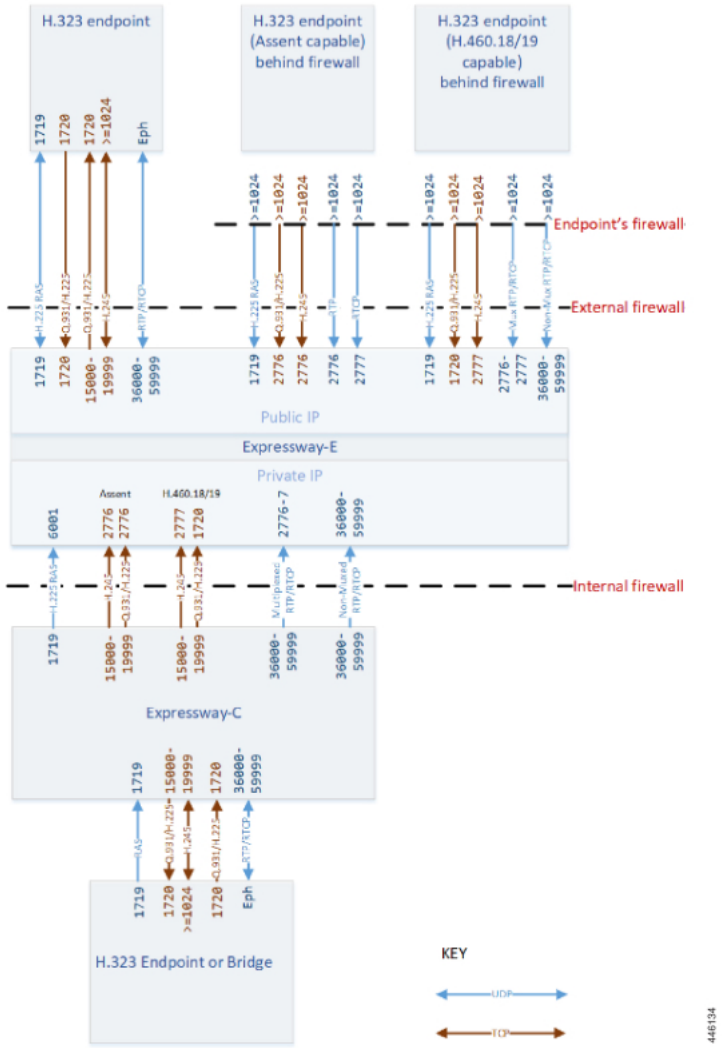
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
承認 RTP（トラバースされたメディア）	SIP エンドポイント（またはそのファイアウォール）	>=1024 エンドポイントポートではなく、メディアが出力されたファイアウォールポートである可能性があります	UDP	Expressway-E	36000 ～ 59999
承認 RTCP（トラバースされたメディア）	SIP エンドポイント（またはそのファイアウォール）	>=1024 ファイアウォールによって、エンドポイントポートではなく、メディアが出力されるポートに変換される可能性があります	UDP	Expressway-E	36000 ～ 59999
承認 RTP（トラバースされたメディア）	Expressway-E	36000 ～ 59999	UDP	SIP エンドポイント（またはそのファイアウォール）	>=1024 Expressway はメディアを受信するまで待機し、その送信元ポート（エンドポイントポートではなく、メディアがファイアウォールを出たポートである可能性があります）にメディアを送信します。

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN 制御	任意の IP アドレス†	>=1024（エンドポイントまたはファイアウォールからのシグナリングポート）	UDP & TCP	Expressway-E	3478（小規模/中規模） 3478 ～ 3483（大規模）
TURN 制御	Expressway-C	>=1024	UDP & TCP	Expressway-E	3478（小規模/中規模） 3478 ～ 3483（大規模）
TURN メディア	Expressway-E	24000 ～ 29999	UDP & TCP	任意の IP アドレス	>=1024
TURN メディア	任意の IP アドレス‡	>=1024 関連する ICE 候補のポート：ホスト IP ポート、サーバー再帰ポート（外部ファイアウォールポート）、または TURN サーバーポート	UDP & TCP	Expressway-E	24000 ～ 29999

† リクエストは、TURN サーバーに認識されていない任意の IP アドレスから送信される可能性があります。たとえば、エンドポイント A とエンドポイント C（TURN クライアント）が Expressway-E TURN サーバーを使用できるとします。TURN サーバーがリクエストを受信する実際の IP アドレスは、エンドポイントのファイアウォール出力アドレス（NATed）である可能性があります。

メディアは、候補アドレスのいずれかに移動できます。たとえば、ICE ネゴシエーションの前に、TURN サーバーはエンドポイント B のどの候補アドレスが最も高い優先順位になるかを認識していません。

H.323 コール


H.323 endpoint
H.323 endpoint (Assent capable) behind firewall
H.323 endpoint (H.460.18/19 capable) behind firewall
Endpoint's firewall
External firewall
Public IP
Expressway-E
Private IP
Assent
H.460.18/19
Internal firewall
Expressway-C
H.323 Endpoint or Bridge
KEY
UDP
TCP
446134

H.323 コールポートリファレンス

表 *12 : H.323* ポートリファレンス

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
初期 RAS 接続	インターネットにエンドポイントを登録	1719	UDP	Expressway-E（パブリック）	1719
初期 RAS 接続	Expressway-E（パブリック）	1719	UDP	インターネットにエンドポイントを登録	1719
初期 RAS 接続	オフプレミスのエンドポイントを保護するファイアウォールの外部アドレス	>=1024	UDP	Expressway-E（パブリック）	1719
初期 RAS 接続	Expressway-C	1719	UDP	Expressway-E プライベート	6001（最初のトラバーサルゾーンの場合。2 番目の場合は 6002 など）
Q.931/H.225 シグナリング	任意（インターネット内のエンドポイント）	1720	TCP	Expressway-E（パブリック）	1720
Q.931/H.225 シグナリング	オフプレミスの承認エンドポイントを保護するファイアウォールの外部アドレス	>=1024	TCP	Expressway-E（パブリック）	2776

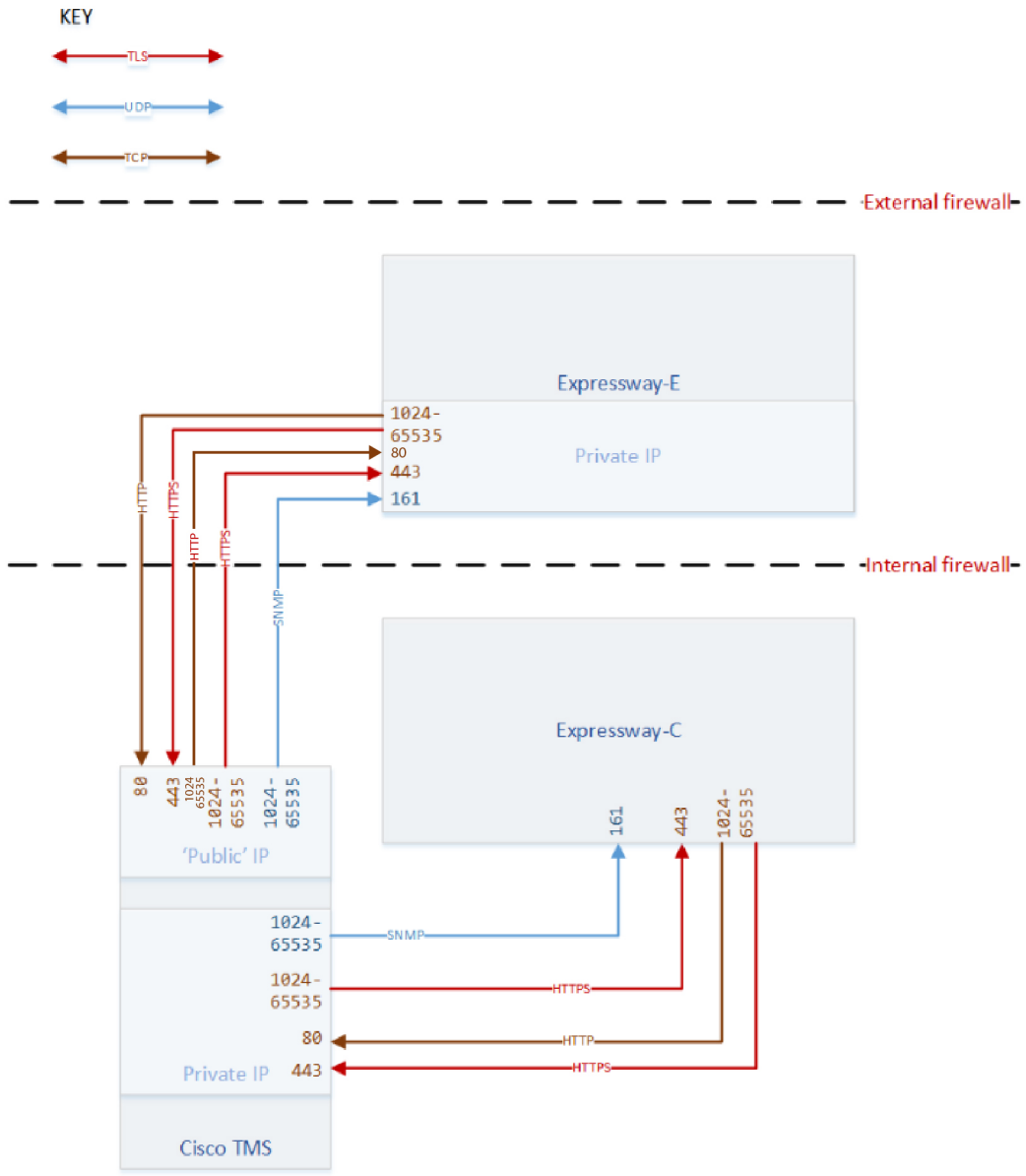
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Q.931/H.225 シグナリング	オフプレミスの H.460.18/19 エンドポイントを保護するファイアウォールの外部アドレス	>=1024	TCP	Expressway-E（パブリック）	1720
Q.931/H.225 シグナリング	Expressway-E（パブリック）	15000 ～ 19999	TCP	任意（インターネット内のエンドポイント）	1720（登録時に指定されたエンドポイント シグナリング ポート。別のポートである可能性があります。1024 以上）
Q.931/H.225 シグナリング	Expressway-C	15000 ～ 19999	TCP	Expressway-E プライベート	2776（承認コール）
Q.931/H.225 シグナリング	Expressway-C	15000 ～ 19999	TCP	Expressway-E プライベート	1720（H.460.18 コール）
H.245	Expressway-C	15000 ～ 19999	TCP	Expressway-E プライベート	2776（承認コール）
H.245	Expressway-C	15000 ～ 19999	TCP	Expressway-E プライベート	2777（H.460.18 コール）
H.245	任意（インターネット内のエンドポイント）	>=1024	TCP	Expressway-E（パブリック）	15000 ～ 19999
H.245	Expressway-E（パブリック）	15000 ～ 19999	TCP	任意（インターネット内のエンドポイント）	>=1024（エンドポイント H.245 シグナリング ポート）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
H.245	オフプレミスの承認エンドポイントを保護するファイアウォールの外部アドレス	>=1024	TCP	Expressway-E（パブリック）	2776
H.245	オフプレミスの H.460.18/19 エンドポイントを保護するファイアウォールの外部アドレス	>=1024	TCP	Expressway-E（パブリック）	2777
RTP（多重化トラバーサルメディア）	Expressway-C	36000 ～ 59998（偶数ポート）	UDP	Expressway-E プライベート	2776（小規模/中規模） または 36000 ～ 36010（偶数ポート）（大規模）
RTCP（多重化トラバーサルメディア）	Expressway-C	36001 ～ 59999（奇数ポート）	UDP	Expressway-E プライベート	2777（小規模/中規模） または 36001 ～ 36011（奇数ポート）（大規模）
RTP（非多重化トラバーサル メディア）	Expressway-C	36000 ～ 59998（偶数ポート）	UDP	Expressway-E プライベート	36000 ～ 59998（偶数ポート）
RTCP（非多重化トラバーサルメディア）	Expressway-C	36001 ～ 59999（奇数ポート）	UDP	Expressway-E プライベート	36001 ～ 59999（奇数ポート）
RTP（非多重化）	Expressway-E（パブリック）	36000 ～ 59998（偶数ポート）	UDP	任意（インターネット内のエンドポイント）	1024 以上（エンドポイントメディア範囲）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
RTCP（非多重化）	Expressway-E（パブリック）	36001 ～ 59999（奇数ポート）	UDP	任意（インターネット内のエンドポイント）	1024 以上（エンドポイントメディア範囲）
RTP（非多重化）	任意（インターネット内のエンドポイント）	1024 以上（エンドポイントメディア範囲）	UDP	Expressway-E（パブリック）	36000 ～ 59998（偶数ポート）
RTCP（非多重化）	任意（インターネット内のエンドポイント）	1024 以上（エンドポイントメディア範囲）	UDP	Expressway-E（パブリック）	36001 ～ 59999（奇数ポート）
RTP（多重化トラバーサルメディア）	オフプレミスの H.460 エンドポイントを保護するファイアウォールの外部アドレス（多重化メディア）	>=1024	UDP	Expressway-E（パブリック）	2776（小規模/中規模） または 36000 ～ 36010（偶数ポート）（大規模）
RTCP（多重化トラバーサルメディア）	オフプレミスの H.460 エンドポイントを保護するファイアウォールの外部アドレス（多重化メディア）	>=1024	UDP	Expressway-E（パブリック）	2777（小規模/中規模） または 36001 ～ 36011（奇数ポート）（大規模）
RTP（多重化トラバーサルメディア）	オフプレミスの H.460 エンドポイントを保護するファイアウォールの外部アドレス（非多重化メディア）	>=1024	UDP	Expressway-E（パブリック）	36000 ～ 59998（偶数ポート）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
RTCP（多重化トラバーサルメディア）	オフプレミスの H.460 エンドポイントを保護するファイアウォールの外部アドレス（非多重化メディア）	>=1024	UDP	Expressway-E（パブリック）	36001 ～ 59999（奇数ポート）

TMS 接続



TMS ポートリファレンス

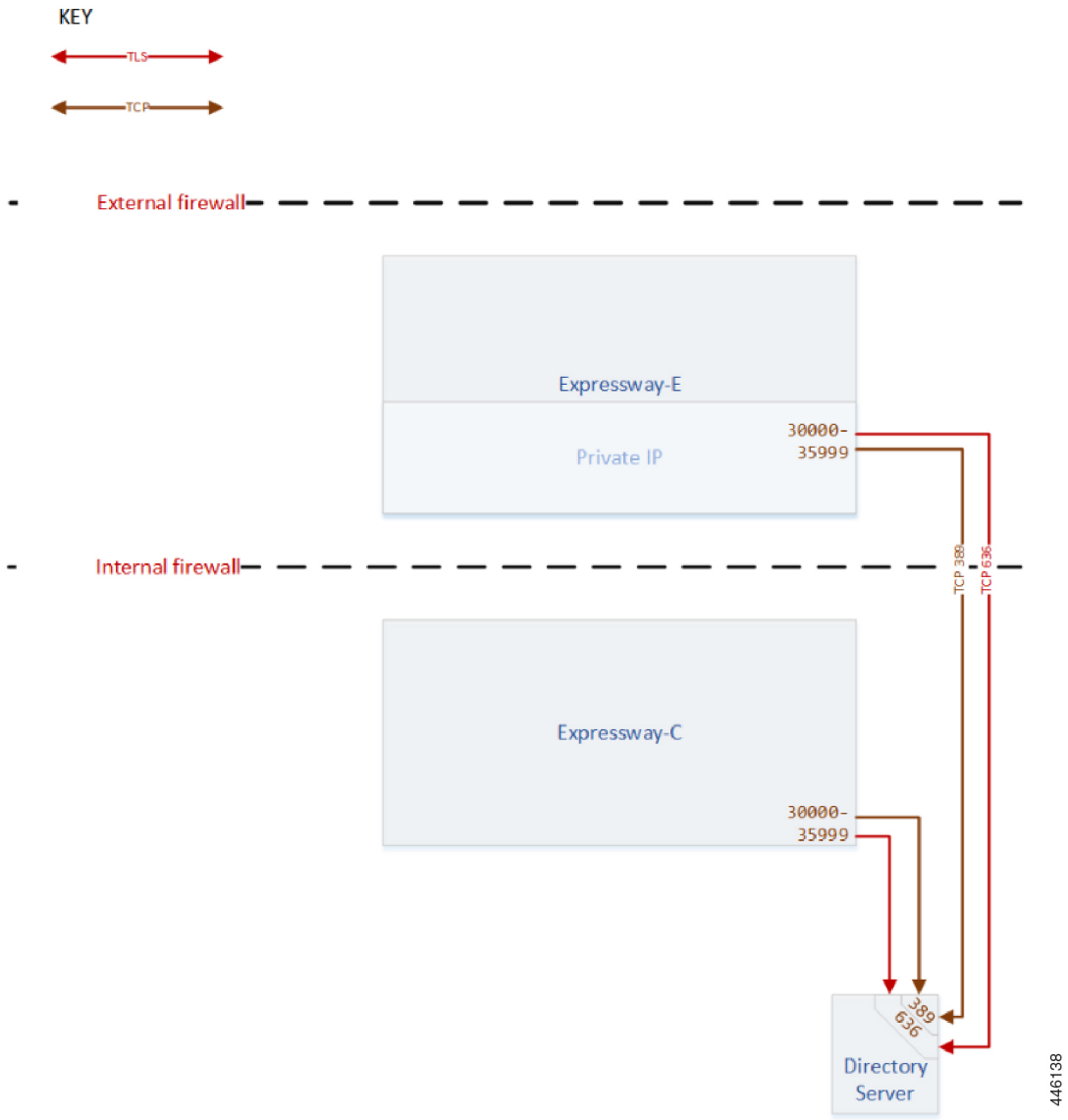
Cisco TMS は、パブリックシステムの管理、または LAN 上のシステムの管理という 2 つの IP アドレスを持つことができます。Cisco TMS で、**[管理ツール（Administrative Tools）]** > **[構成（Configuration）]** > **[ネットワーク設定（Network Settings）]** > **[詳細ネットワーク設定**

（**Advanced Network Settings**）] に移動します。Expressway-E では TMS パブリックアドレスを使用し、Expressway-C ではデフォルト LAN アドレスを使用する必要があります。

表 *13 : TMS* ポートリファレンス

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Expressway-E の検出のための SNMP	Cisco TMS 外部 IP	1024 ～ 65535	UDP	Expressway-E プライベート	161
Expressway-C の検出のための SNMP	Cisco TMS	1024 ～ 65535	UDP	Expressway-C	161
Expressway-E の HTTP 管理	Cisco TMS 外部 IP	1024 ～ 65535	TCP	Expressway-E プライベート IP	80
Expressway-C の HTTP 管理	Cisco TMS	1024 ～ 65535	TCP	Expressway-E プライベート IP	80
Expressway-E の HTTPS 管理	Cisco TMS 外部 IP	1024 ～ 65535	TLS	Expressway-E プライベート	443
Expressway-C の HTTPS 管理	Cisco TMS	1024 ～ 65535	TLS	Expressway-C	443
フィードバックイベント（HTTP）	Expressway-E プライベート	1024 ～ 65535	TCP	Cisco TMS 外部 IP	80
フィードバックイベント（HTTP）	Expressway-C	1024 ～ 65535	TCP	Cisco TMS	80
フィードバックイベント（HTTPS）	Expressway-E プライベート	1024 ～ 65535	TLS	Cisco TMS 外部 IP	443
フィードバックイベント（HTTPS）	Expressway-C	1024 ～ 65535	TLS	Cisco TMS	443

LDAP 接続

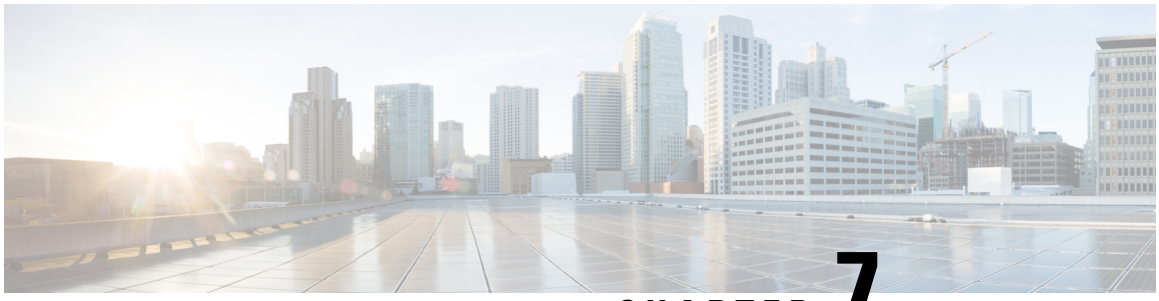


LDAP ポート リファレンス

LDAP サーバーを使用して、管理者またはユーザーのログインを認証および許可することを選択できます。Expressway-E から着信する LDAP ポートを許可する必要があるのは、ユーザーがネットワークの外部からログインする必要があり、クレデンシャルを Expressway に保存しないというまれなケースです。

表 *14 : LDAP* ポート リファレンス

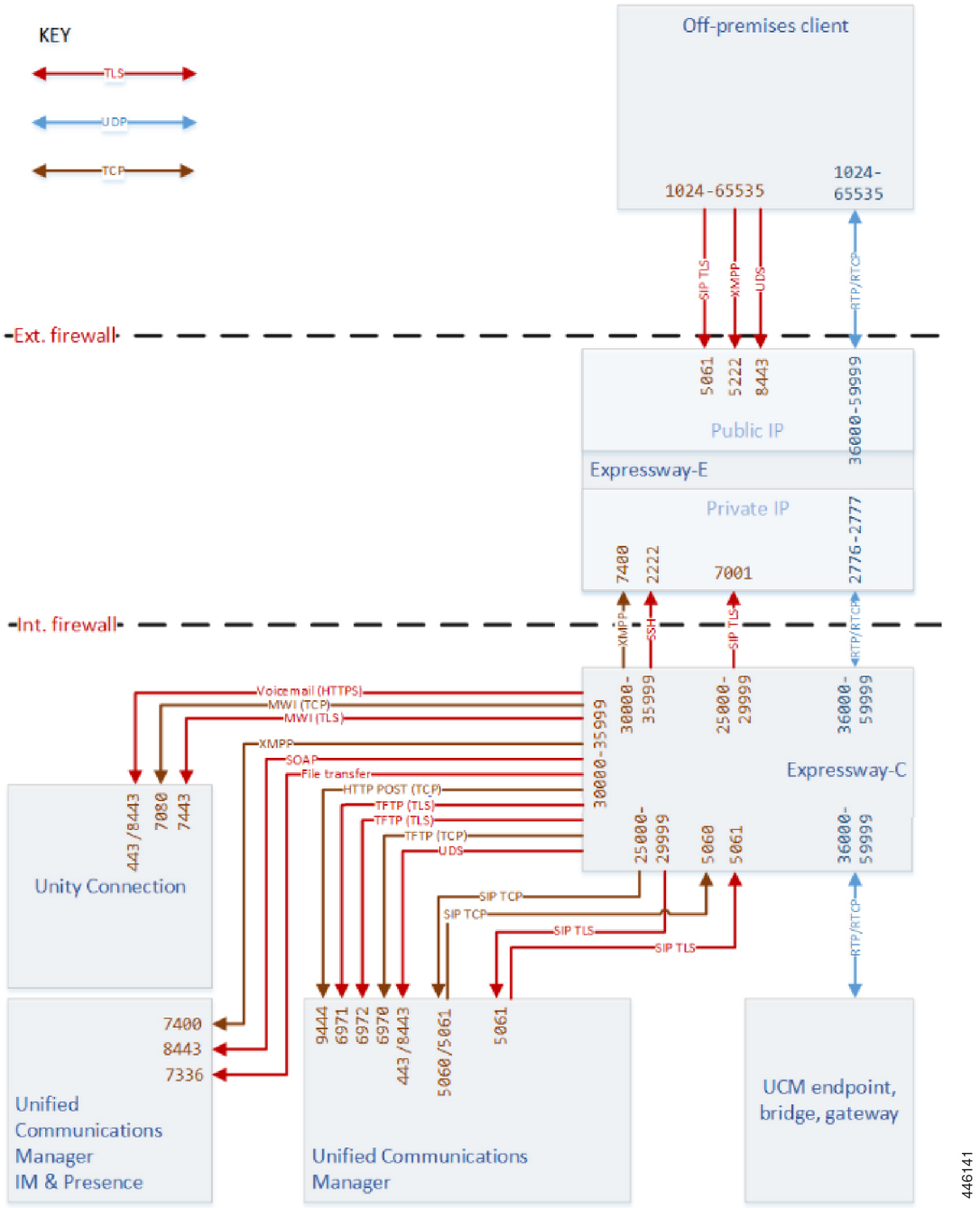
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Expressway-C からの認証リクエスト	Expressway-C	30000 ～ 35999	TCP	ディレクトリサーバー	389
Expressway-E からの認証リクエスト	Expressway-E プライベート	30000 ～ 35999	TCP	ディレクトリサーバー	389
Expressway-C からの暗号化された認証リクエスト	Expressway-C	30000 ～ 35999	TLS	ディレクトリサーバー	636
Expressway-E からの暗号化された認証リクエスト	Expressway-E プライベート	30000 ～ 35999	TLS	ディレクトリサーバー	636



CHAPTER 7

モバイル & リモート アクセス

MRA 接続


KEY
TLS
UDP
TCP
Off-premises client
1024-65535
1024-65535
SIP TLS
XMPP
UDS
RTP/RTCP
Ext. firewall
5061
5222
8443
36000-59999
Public IP
Expressway-E
Private IP
7400
2222
7001
2776-2777
Int. firewall
XMPP
SSH
SIP TLS
RTP/RTCP
Voicemail (HTTPS)
MWI (TCP)
MWI (TLS)
XMPP
SOAP
File transfer
HTTP POST (TCP)
TFTP (TLS)
TFTP (TLS)
TFTP (TCP)
UDS
30000-35999
30000-35999
25000-29999
36000-59999
Expressway-C
25000-29999
5060
5061
36000-59999
SIP TCP
SIP TCP
SIP TLS
SIP TLS
RTP/RTCP
443/8443
7080
7443
Unity Connection
7400
8443
7336
Unified Communications Manager IM & Presence
9444
6971
6972
6970
443/8443
5060/5061
5061
Unified Communications Manager
UCM endpoint, bridge, gateway
446141

MRA ポートリファレンス

表 *15*：オフプレミスエンドポイント間の *ICE* パススルー接続

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
RTP/RTCP（ICE パススルーメディア）†	オフプレミスのエンドポイント	Eph	UDP	オフプレミスのエンドポイント	Eph

† ICE パススルーコールは、オフプレミスのエンドポイント間でのみサポートされます。オフプレミスとオンプレミスのエンドポイント間ではサポートされていません。

表 *16*：オフプレミスエンドポイントと *Expressway-E* 間の接続

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
UDS（電話帳およびプロビジョニング）	オフプレミスのエンドポイント	1024 ～ 65535	TLS	Expressway-E パブリック IP	8443
SIP シグナリング	オフプレミスのエンドポイント	1024 ～ 65535	TLS	Expressway-E パブリック IP	5061
RTP/RTCP メディア	オフプレミスのエンドポイント	1024 ～ 65535	UDP	Expressway-E パブリック IP	36000 ～ 59999
RTP/RTCP メディア	Expressway-E パブリック IP	36000 ～ 59999	UDP	オフプレミスのエンドポイント	1024 ～ 65535
XMPP（IM and Presence）	オフプレミスのエンドポイント	1024 ～ 65535	TCP	Expressway-E パブリック IP	5222
TURN 制御（ICE パススルー）	任意の IP アドレス†	>=1024（エンドポイントまたはファイアウォールからのシグナリングポート）	UDP	Expressway-E	3478（小規模/中規模） 3478 ～ 3483（大規模）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN メディア（ICE パススルー）	任意の IP アドレス‡	>=1024 関連する ICE 候補のポート：ホスト IP ポート、サーバー再帰ポート（外部ファイアウォールポート）、または TURN サーバーポート	UDP	Expressway-E	24000 ～ 29999

† リクエストは、TURN サーバーに認識されていない任意の IP アドレスから送信される可能性があります。たとえば、エンドポイント A とエンドポイント B（TURN クライアント）が Expressway-E TURN サーバーを使用できるとします。TURN サーバーがリクエストを受信する実際の IP アドレスは、エンドポイントのファイアウォール出力アドレス（NATed）である可能性があります。

メディアは、候補アドレスのいずれかに移動できます。たとえば、ICE パススルーネゴシエーションの前に、TURN サーバーはエンドポイント B のどの候補アドレスが最も優先順位が高いかを認識しません。

表 *17 : Expressway-C* と *Expressway-E* 間の接続

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SSH トンネル	Expressway-C	30000 ～ 35999	TLS	Expressway-E プライベート IP	2222
SIP シグナリング	Expressway-C	25000 ～ 29999	TLS	Expressway-E プライベート IP	7001
SIP メディア	Expressway-C	36000 ～ 59999	UDP	Expressway-E プライベート IP	2776/7 または 36000-11
XMPP（IM and Presence）	Expressway-C	30000 ～ 35999	TCP	Expressway-E プライベート IP	7400

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN 制御	Expressway-C	>=1024	UDP & TCP	Expressway-E	3478（小規模/中規模） 3478 ～ 3483（大規模）

表 *18 : Expressway-C* とオンプレミス インフラストラクチャ間の接続

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP シグナリング（TCP）	Expressway-C	25000 ～ 29999	TCP	Unified CM	5060†
SIP シグナリング（TCP）	Unified CM	エフェメラル	TCP	Expressway-C	[5060]
SIP シグナリング（TLS）	Expressway-C	25000 ～ 29999	TLS	Unified CM	5061*
SIP シグナリング（TLS）	Unified CM	エフェメラル	TLS	Expressway-C	5061
SIP シグナリング（OAuth）	Expressway-C	25000 ～ 29999	TLS	Unified CM	5091
SIP シグナリング（OAuth）	Unified CM	5091	TLS	Expressway-C	5061
HTTP コンフィギュレーション ファイルのダウンロード（TFTP） （11.x より前の Jabber および 11.x より前の Unified CM）	Expressway-C	30000 ～ 35999	TCP	Unified CM ノード	6970

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
HTTPS ヘッドセット設定ファイルのダウンロード（TFTP）	Expressway-C	30000 ～ 35999	TLS	Unified CM	6971
HTTPS コンフィギュレーション ファイルのダウンロード（TFTP） （11.x 以降の Jabber および 11.x 以降の Unified CM）	Expressway-C	30000 ～ 35999	TLS	Unified CM ノード	6972
UDS（ユーザーデータサービス）および AXL（Administrative XML Layer）の HTTP	Expressway-C	30000 ～ 35999	TLS	Unified CM ノード	443 または 8443
XMPP（IM and Presence）	Expressway-C	30000 ～ 35999	TLS	IM and Presence Service ノード	7400
HTTPS SOAP（IM and Presence）	Expressway-C	30000 ～ 35999	TLS	IM and Presence Service ノード	8443
ファイル転送（IM and Presence）	Expressway-C	30000 ～ 35999	TLS	IM and Presence Service ノード	7336
HTTPS からビジュアルボイスメール	Expressway-C	30000 ～ 35999	TLS	Cisco Unity Connection	443 または 8443
MWI（メッセージ受信インジケータ）	Expressway-C	30000 ～ 35999	TCP	Cisco Unity Connection	7080

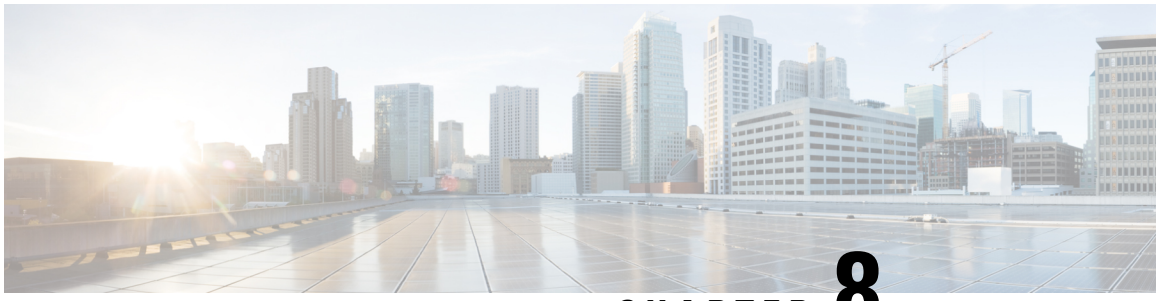
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
MWI（メッセージ受信インジケータ）	Expressway-C	30000 ～ 35999	TLS	Cisco Unity Connection	7443
メトリック POST の HTTP（ヘッドセット管理）	Expressway-C	30000 ～ 35999	TCP	Unified CM	9444
オーディオビデオメディア（RTP/RTCP）	Expressway-C	36000 ～ 59999	UDP	オンプレミスのメディア接続先	宛先メディアの範囲（例：16384-32767（DX シリーズ））

† Unified CM は 5061 で TCP SIP をリッスンできますが、推奨されません。

* 5060/5061 への回線側接続である Unified CM への MRA 接続がある場合は、その Unified CM で作成する SIP トランクのリスニングポートとして 5060/5061 を使用しないでください。

表 *19 : Expressway-E* からクラウドへの接続

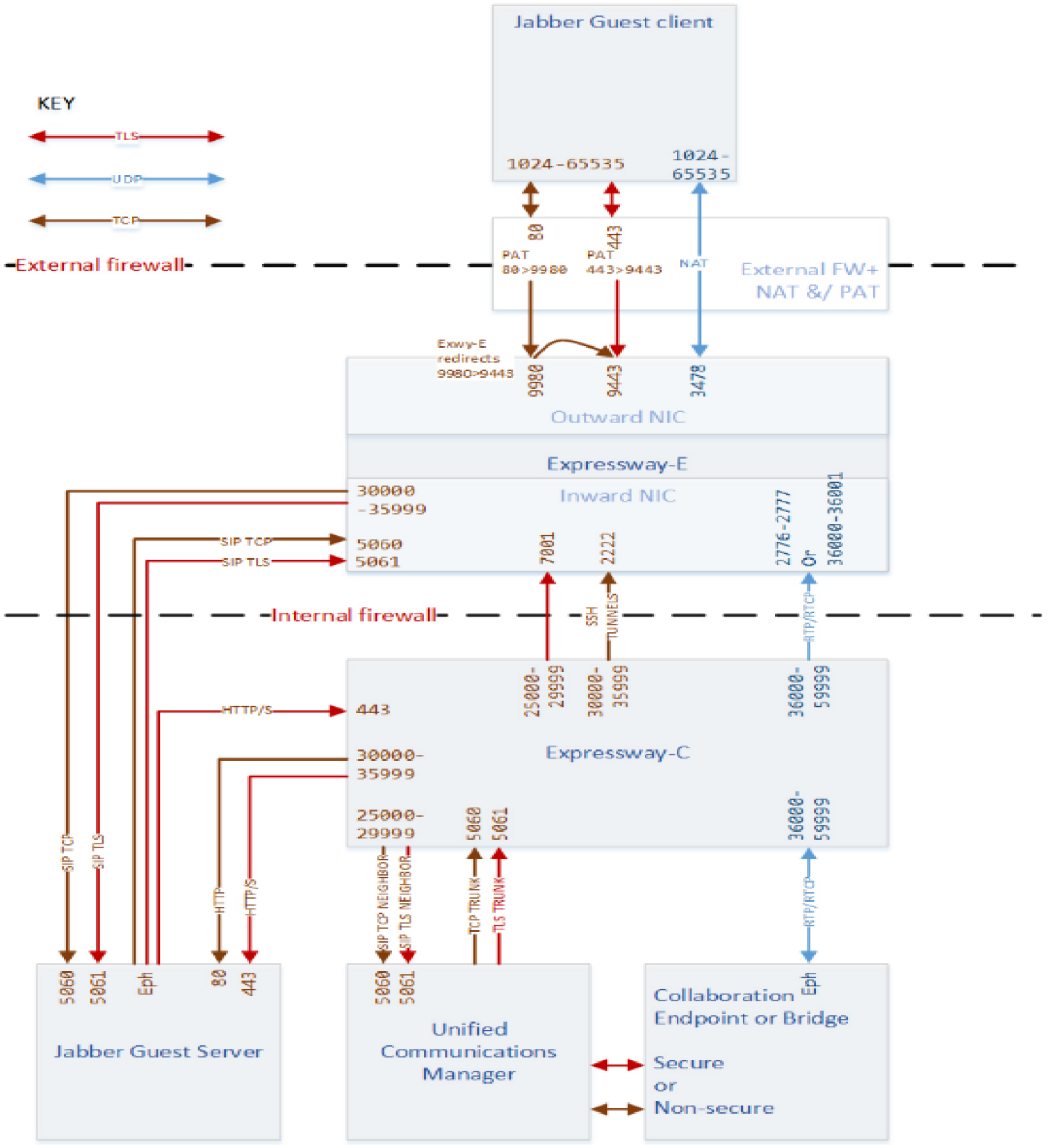
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Unified CM から発信されるサブスクリプションリクエスト	Expressway-E	エフェメラル（30000 ～ 35999）	TLS	fos-a.wbx2.com（オンボーディングサービス）	443
Unified CM または IM and Presence Service から発信される認証リクエスト	Expressway-E	エフェメラル（30000 ～ 35999）	TLS	idbroker。 webex.com （共通アイデンティティサービス）	443



CHAPTER 8

Jabber Guest サービス

Jabber Guest：デュアル NIC 展開



Jabber Guest：デュアル NIC 展開ポート

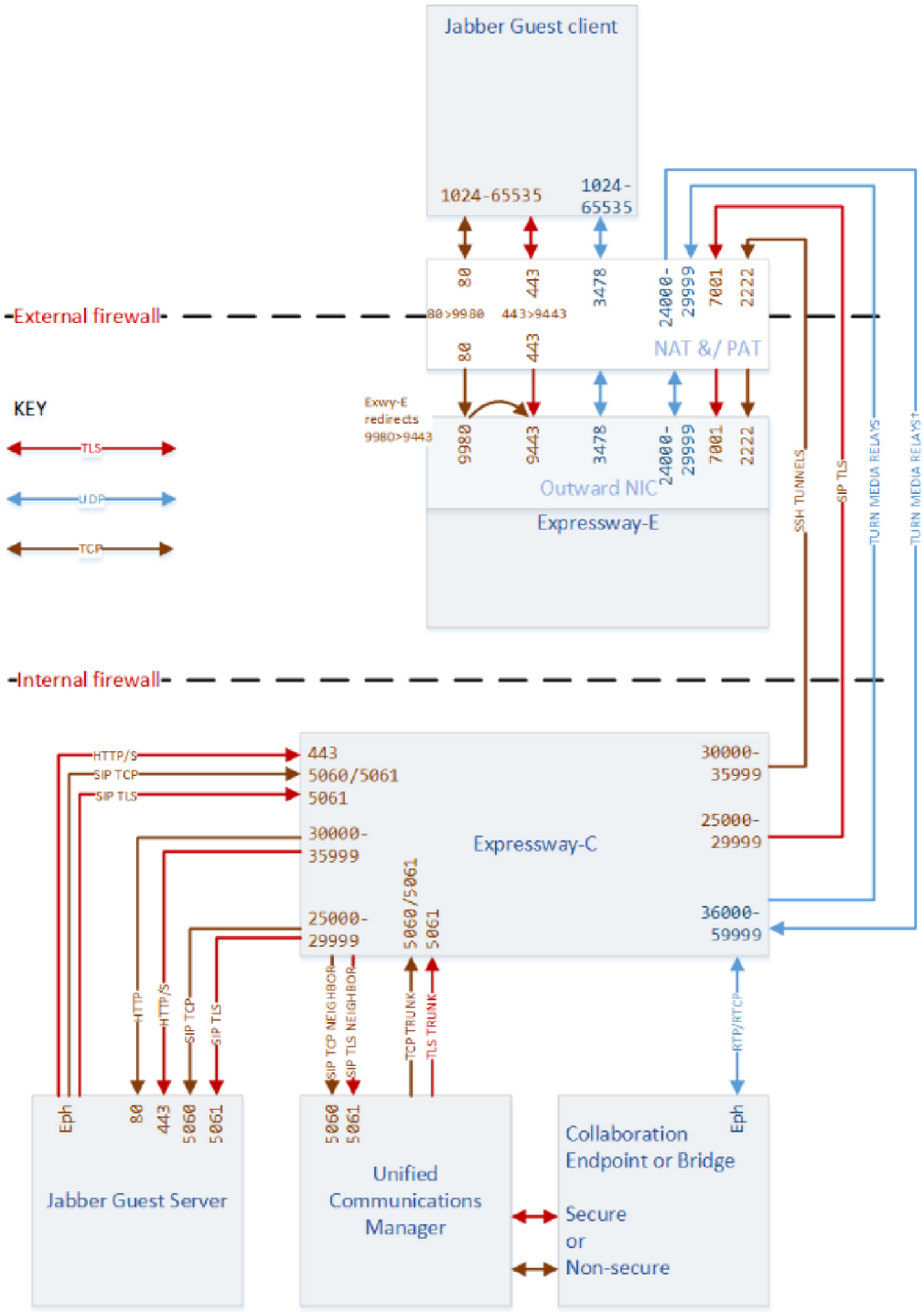
表 *20 : Jabber Guest* デュアル *NIC* 展開のポートリファレンス

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Jabber Guest クライアントシグナリング（HTTP は常に HTTPS にリダイレクト）	任意（Web ブラウザ）	1024 ～ 65535	TCP	Expressway-E パブリック IP	80
Jabber Guest クライアント セキュア シグナリング（HTTPS）	任意（Web ブラウザ）	1024 ～ 65535	TLS	Expressway-E パブリック IP	443
ポートの競合を回避するために、Expressway-E public:80 へのトラフィックは private:9980 に NAT&PAT する必要があります。HTTP は常に HTTPS にリダイレクトされます。			TLS	Expressway-E プライベート IP （外部 NIC）	9980 [#1]
ポートの競合を回避するために、Expressway-E public:443 へのトラフィックは、private:9443 に NAT&PAT する必要があります。			TLS	Expressway-E プライベート IP （外部 NIC）	9443 [#2]
Jabber Guest クライアントメディア（TURN）	任意（Web ブラウザ）	1024 ～ 65535	UDP	Expressway-E パブリック IP	3478（S/M システム） 3478 ～ 3483（L システム）[*3] を参照してください（欠落または誤って切り取り）
SIP TCP シグナリング	Expressway-E プライベート IP	30000 ～ 35999	TCP	Jabber Guest サーバー	[5060]

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP TLS シグナリング	Expressway-E プライベート IP	30000 ～ 35999	TLS	Jabber Guest サーバー	5061
SIP TCP シグナリング	Jabber Guest サーバー	Eph	TCP	Expressway-E プライベート IP	[5060]
SIP TLS シグナリング	Jabber Guest サーバー	Eph	TLS	Expressway-E プライベート IP	5061
多重化メディアトラバーサル	Expressway-C	36000 ～ 59999	UDP	Expressway-E 内部 NIC	2776 ～ 2777 または 36000 ～ 36001

[1] ポート変換が必要
[2] ポート変換が必要
[3] 大規模システムでは、TURN リクエストリスニング ポートの範囲を設定できます。デフォルトのポート範囲は 3478 ～ 3483 です。大規模システムでは、ポート多重化が有効になっている場合、TURN リクエスト用に単一のポートを設定できます。TURN ポートの多重化の詳細については、

Jabber Guest：単一 NIC 展開



Jabber Guest：単一 NIC 展開ポート

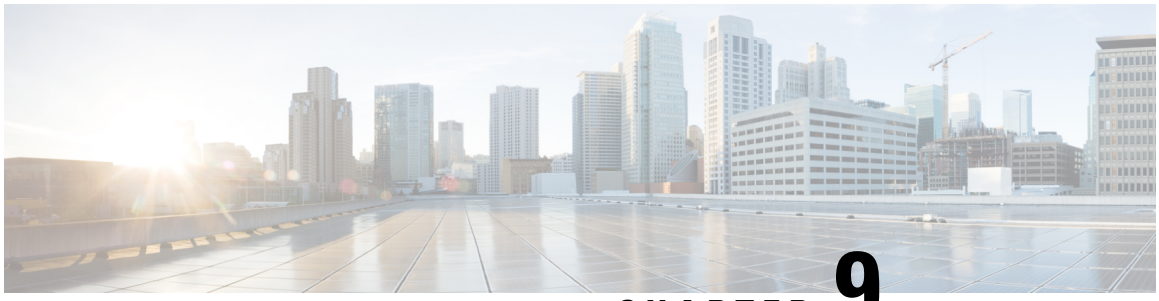
表 *21 : Jabber Guest* 単一 *NIC* 展開のポートリファレンス

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Jabber Guest クライアントメディア（TURN）	いずれか（Any）	1024 ～ 65535	UDP	Expressway-E パブリック IP	3478（S/M システム） 3478 ～ 3483（L システム）*4
Jabber Guest クライアントシグナリング（HTTP は常に HTTPS にリダイレクト）	いずれか（Any）	1024 ～ 65535	TCP	Expressway-E パブリック IP	80
Jabber Guest クライアント セキュア シグナリング（HTTPS）	いずれか（Any）	1024 ～ 65535	TLS	Expressway-E パブリック IP	443
ポートの競合を回避するために、Expressway-E public:80 へのトラフィックは private:9980 に NAT&PAT する必要があります。HTTP は常に HTTPS にリダイレクトされます。			TLS	Expressway-E プライベート IP	9980 #5
ポートの競合を回避するために、Expressway-E public:443 へのトラフィックは、private:9443 に NAT&PAT する必要があります。			TLS	Expressway-E プライベート IP	9443 #6
Expressway-C から Expressway-E への SSH トンネル	Expressway-C	35000 ～ 35999	TCP	Expressway-E パブリック IP	2222
SIP シグナリング	Expressway-C	25000 ～ 25999	TLS	Expressway-E パブリック IP	7001
TURN メディアリレー	Expressway-C	36000 ～ 59999	UDP	Expressway-E パブリック IP	24000 ～ 29999

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN メディアリレー**[7]	Expressway-E パブリック IP	24000 ～ 29999	UDP	Expressway-C	36000 ～ 59999
SIP TCP シグナリング	Expressway-C	30000 ～ 35999	TCP	Jabber Guest サーバー	[5060]
SIP TLS シグナリング	Expressway-C	30000 ～ 35999	TLS	Jabber Guest サーバー	5061
SIP TCP シグナリング	Jabber Guest サーバー	Eph	TCP	Expressway-C	[5060]
SIP TLS シグナリング	Jabber Guest サーバー	Eph	TLS	Expressway-C	5061

[4] 大規模システムでは、TURN リクエストリスニングポートの範囲を設定できます。デフォルトのポート範囲は 3478 ～ 3483 です。
[5] 外部ファイアウォールでのポート変換
[6] 外部ファイアウォールでのポート変換
[7] インバウンドメディアポートは、Jabber Guest クライアントから開始された単方向メディアにのみ必要です（BFCP など）。それ以外の場合は、Expressway-C から Expressway-E までのアウトバウンドメディア範囲を許可するだけで十分です（前の行）。

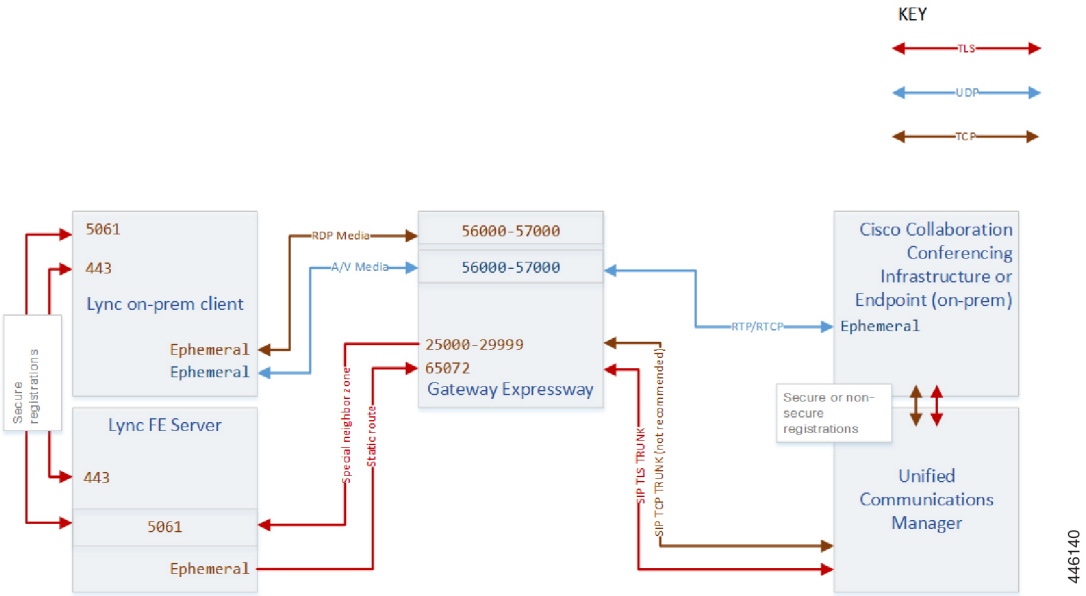
（注） 単一の NIC 展開を使用している場合、コアとエッジ間の通信は NAT リフレクションを使用する必要がありますが、コアからエッジへの宛先 IP はパブリックになります。



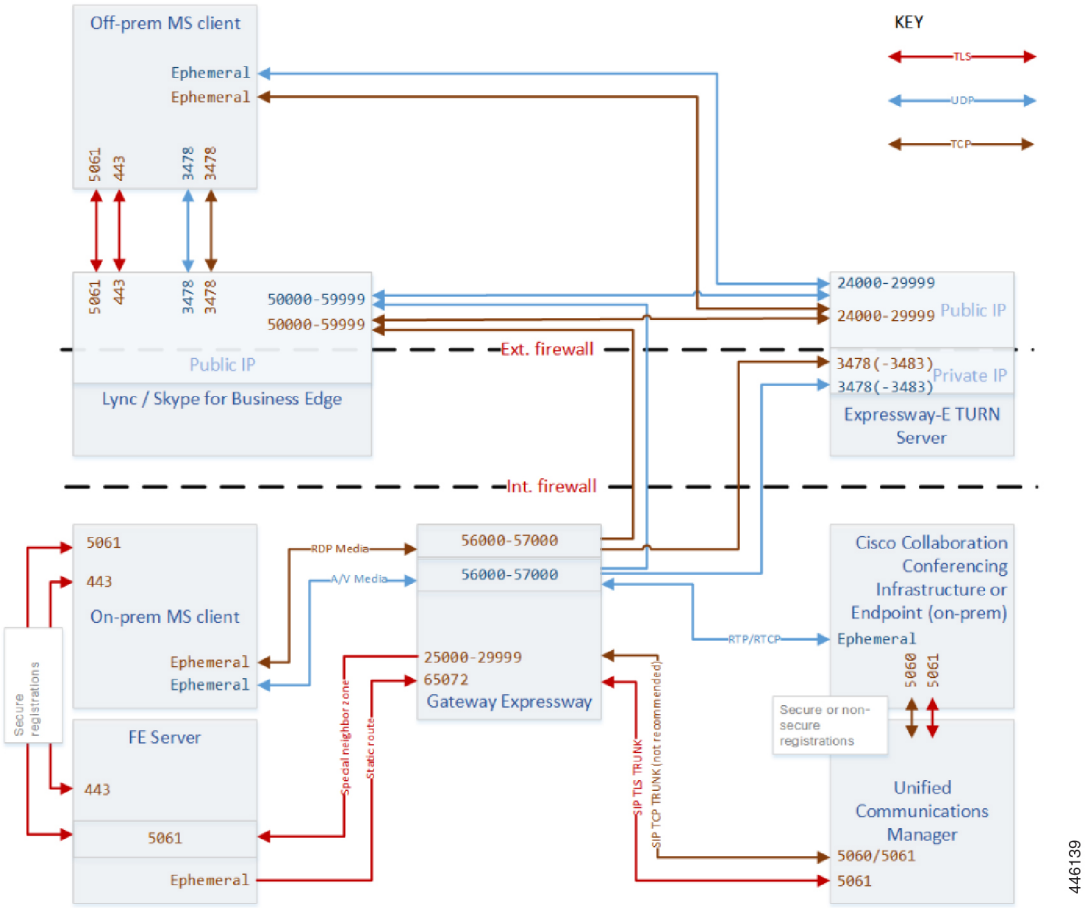
CHAPTER 9

Gateway Expressway を使用した Microsoft の相互運用性

オンプレミスの Microsoft クライアント



オフプレミスの Microsoft クライアント



Microsoft インフラストラクチャ ポート リファレンスを使用した Expressway

展開接続とポートについて

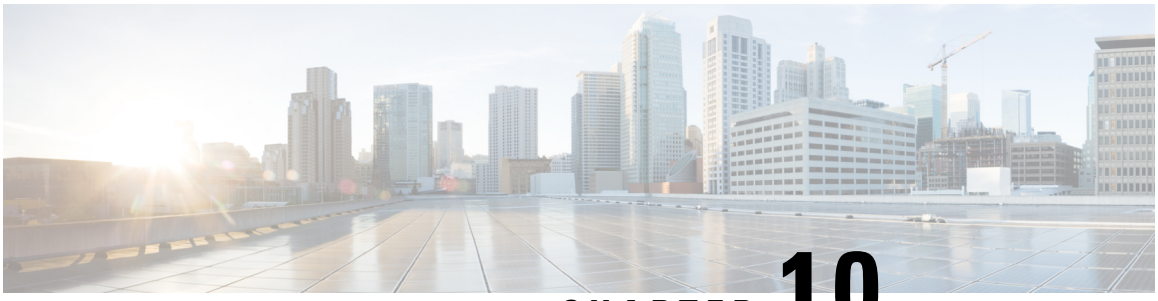
- Microsoft インフラストラクチャ要素間のトランク接続は表示されません。
- Microsoft クライアントからクライアントへのコールに必要なメディア/シグナリング接続は示されていません。
- Microsoft のポート範囲は、ここに示すものとは異なる場合があります。インフラストラクチャに定義されているポート範囲を確認するには、Microsoft のドキュメントを確認してください。

- Cisco Unified Communications Manager とコラボレーション エンドポイントの接続は図示していません（わかりやすくするため）。MRA 接続 （42 ページ） でそれらの例を確認できます。
- DMZ には 2 つの TURN サーバーがあるため、複数のメディアパスが可能です。「任意」の送信元 IP アドレスがリストされています。これは、ICE ネゴシエーションにより、メディアパスが TURN サーバーの 1 つによって提供されるリレーアドレス、またはファイアウォール/NAT の出力側からの再帰アドレスを使用することを意味する可能性があるためです。
- Gateway Expressway の Microsoft 相互運用性サービスには、メディアポートの共有プールがあります（デフォルトは 56000 ～ 57000）。サービスは、TCP または UDP トランスポートのいずれかのメディア接続に、範囲内の任意のポートを使用できます。
- Expressway-E で 1 つまたは 2 つの NIC が有効になっている可能性があるため、図には Expressway-E の 2 つの IP アドレスが示されています。 （Gateway Expressway の Microsoft 相互運用性設定で）TURN サーバー用に入力したアドレスは、3478（TCP および UDP）でリッスンする必要があります。

表 *22 : SIP* シグナリング ポート リファレンス

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Lync 環境への SIP シグナリング	Gateway Expressway	25000 ～ 29999	TLS	Lync FE サーバー	5061
Lync 環境からの SIP シグナリング	Lync FE サーバー	エフェメラル ポート（1024 ～ 65535）	TLS	Gateway Expressway：MS 相互運用性 B2BUA	65072
SIP シグナリング	Microsoft クライアント	5061	MTLS	Microsoft Edge	5061
SIP シグナリング	Microsoft Edge	5061	MTLS	Microsoft クライアント	5061
SIP/TLS および TCP TURN	Microsoft クライアント	443	TLS	Microsoft Edge	443
SIP/TLS および TCP TURN	Microsoft Edge	443	TLS	Microsoft クライアント	443
STUN	Microsoft クライアント	3478	UDP	Microsoft Edge	3478
STUN	Microsoft Edge	3478	UDP	Microsoft クライアント	3478

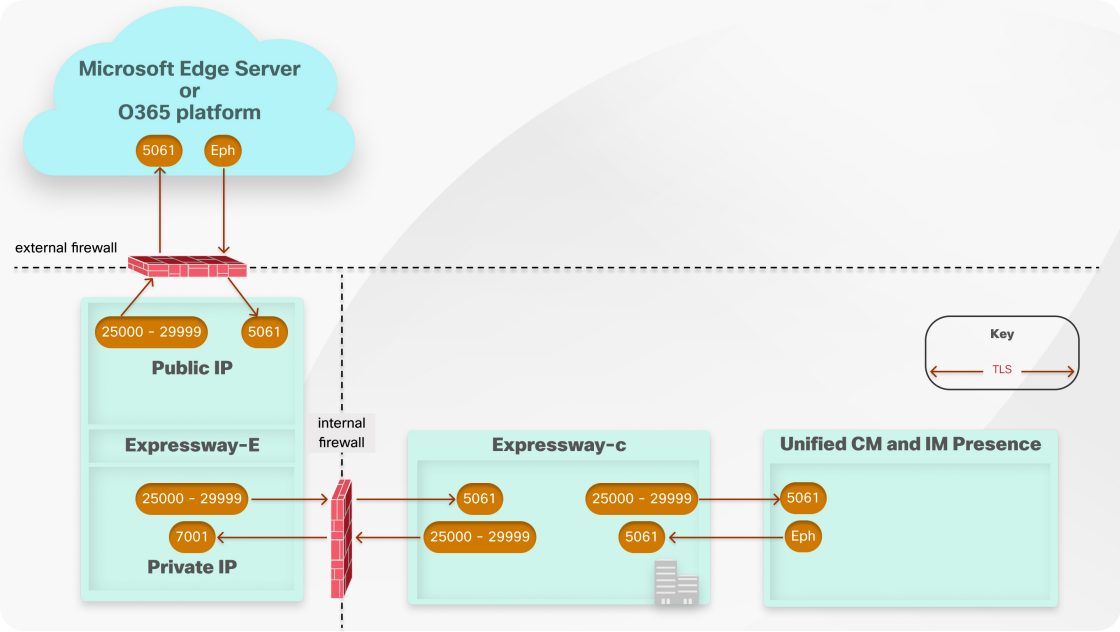
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
AV メディアからオンプレミスの Lync クライアントへ	Gateway Expressway	56000 ～ 57000	UDP	Lync クライアント	Lync クライアントメディアポート
オンプレミスの Lync クライアントからの画面共有	Lync クライアント	443	TCP	Gateway Expressway	56000 ～ 57000
Microsoft 相互運用性 B2BUA からオンプレミスのシスココラボレーション受信者へのメディア	Gateway Expressway	56000 ～ 57000	UDP	展開によって異なります。ブリッジ、エンドポイント、または SIP プロキシ	エンドポイント メディア ポート
Gateway Expressway から Expressway-E TURN サーバーへの ICE ネゴシエーションおよび TURN リクエスト	Gateway Expressway	56000 ～ 57000	UDP または TCP	Expressway-E TURN サーバー	UDP 3478 TCP 3478 （大規模システムの場合は 3478 ～ 3483）
UDP TURN メディアリレー	Expressway-E TURN サーバー	24000 ～ 29999	UDP	MS クライアントまたは Edge からの任意（再帰またはリレー）	50000 ～ 59999（Edge 範囲）またはクライアントメディアポート
TCP TURN メディアリレー	Expressway-E TURN サーバー	24000 ～ 29999	TCP	MS クライアントまたは Edge からの任意（再帰またはリレー）	50000 ～ 59999（Edge 範囲）またはクライアントメディアポート



CHAPTER 10

Microsoft クライアントとの IM and Presence フェデレーション

Microsoft Connections を使用した IM and Presence Service フェデレーション

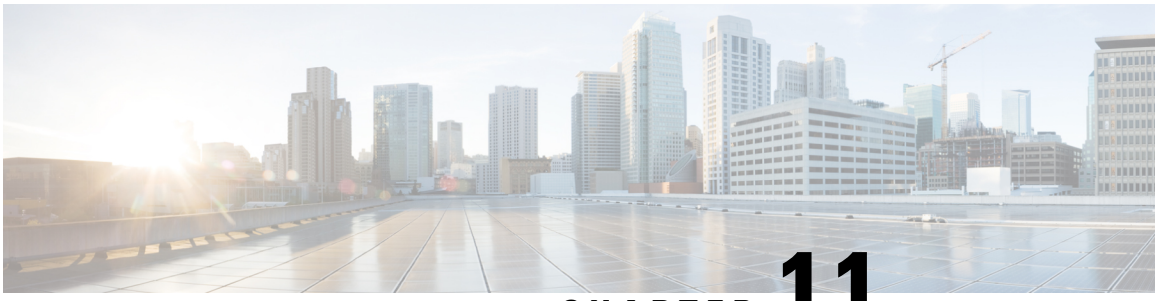


Microsoft クライアント ポート リファレンスを使用した IM and Presence フェデレーション

表 *23 : Microsoft* インフラストラクチャとの *IM and Presence Service* フェデレーション

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Expressway-E はインバウンド Microsoft SIP IM&P をリッスンします	任意（フェデレーテッドドメインの Microsoft インフラストラクチャ）	1024 ～ 65535	TLS	Expressway-E パブリック	5061
Expressway-C はインバウンド Microsoft SIP IM&P をリッスンします	Expressway-E プライベート	25000 ～ 29999	TLS	Expressway-C	5061
IM and Presence Service はインバウンド Microsoft SIP IM&P をリッスンします	Expressway-C	25000 ～ 29999	TLS	IM and Presence Service パブリッシャ	5061
Expressway-C はアウトバウンド Microsoft SIP IM&P をリッスンします	IM and Presence Service パブリッシャ	1024 ～ 65535	TLS	Expressway-C	5061
Expressway-E はアウトバウンド Microsoft SIP IM&P をリッスンします	Expressway-C	25000 ～ 29999	TLS	Expressway-E プライベート	7001（最初のトラバーサルゾーンの場合。2 番目の場合は 7002 など）

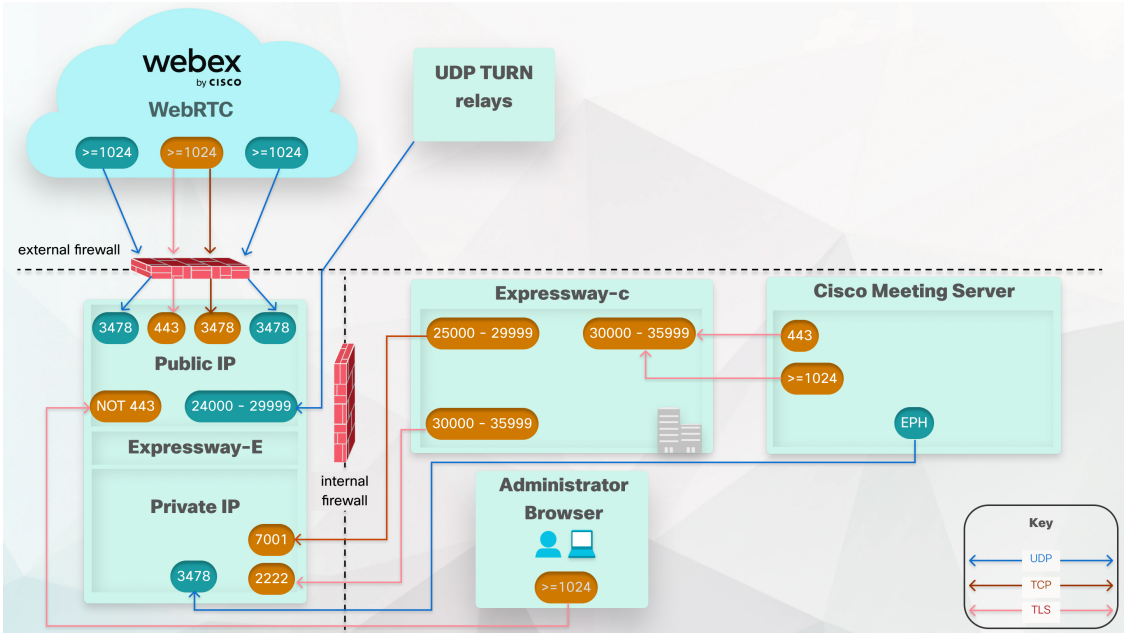
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
Microsoft インフラストラクチャは、インバウンド Microsoft SIP IM&P をリッスンします。	Expressway-E	25000 ～ 29999	TLS	任意（フェデレーテッドドメインの Microsoft インフラストラクチャ）	5061



CHAPTER 11

Cisco Meeting Server

Cisco Meeting Server 接続用 Web プロキシ



Cisco Meeting Server ポートリファレンス用 Web プロキシ

表 *24 : Meeting Server* の *Web* プロキシ

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
CMA Web クライアントシグナリング	ゲスト PC	1024 ～ 65535	TLS	Expressway-E パブリック IP	443 [18]
トンネルメディア	CMA Cisco Meeting WebRTC アプリ	1024 ～ 65535	UDP	Expressway-E パブリック IP	3478（および設定されている場合は TCP オーバーライドポート）
Web インターフェイスアクセス	管理者の PC	1024 ～ 65535	TLS	Expressway-E IP	NOT 443 [29] 8443 [310]

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
ファイアウォール トラバーサル用の SSH トンネル	Expressway-C	30000 ～ 35999	TCP	Expressway-E プライベート IP	2222
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP または TLS	Expressway-E	7001（最初のトラバーサル ゾーンの場合。2 番目の場合は 7002 など）
CMA Cisco Meeting WebRTC アプリ TURN リクエスト	任意のIP	1024 ～ 65535	UDP	Expressway-E TURN サーバーのパブリック IP	3478
CMA Cisco Meeting WebRTC アプリ TURN リクエスト（TCP フォールバック）	任意のIP	1024 ～ 65535	TCP	Expressway-E TURN サーバーのパブリック IP	3478 [411]
Webbridge シグナリング（HTTPS）	Expressway-C	30000 ～ 35999	HTTPS	Meeting Server	443
Webbridge シグナリング（HTTPS）	Meeting Server	>=1024	HTTPS	Expressway-C	30000 ～ 35999
TURN クライアントリクエスト	Meeting Server	1024 ～ 65535	UDP	Expressway-E TURN サーバーのプライベート IP	3478

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN リレー[5][12]	元のソース：Expressway-E プライベート IP 変換後のソース：Expressway-E パブリック IP	24000 ～ 29999	UDP および TCP	元の宛先：Expressway-E パブリック IP 変換後の宛先：Expressway-E プライベート IP	24000 ～ 29999
TURN リレー（オンプレミス）	Expressway-E プライベート IP	24000 ～ 29999	UDP および TCP	Expressway-E プライベート IP	24000 ～ 29999
TURN リレー[6][13]	Meeting Server	エフェメラル	UDP	Expressway-E パブリック IP	24000 ～ 29999

[8] WebRTC クライアントは 443 を使用するため、管理ポートを変更することをお勧めします。WebRTC ブラウザがポート 80 にアクセスしようとすると、Expressway-E は接続を 443 にリダイレクトします。

[9] 代替管理ポートのオプションが Web インターフェイスに表示されます。CLI を使用して別のポートに変更でき（7443 など）、ロックできます。パブリック IP アドレスで外部管理ポートを開くことを強くお勧めします。WebRTC ブラウザがポート 80 にアクセスしようとすると、Expressway-E は接続を 443 にリダイレクトします。

[10] Meeting Server と Expressway の展開が MRA と共存している場合は、Web 管理にポート 8443 を使用しないでください。

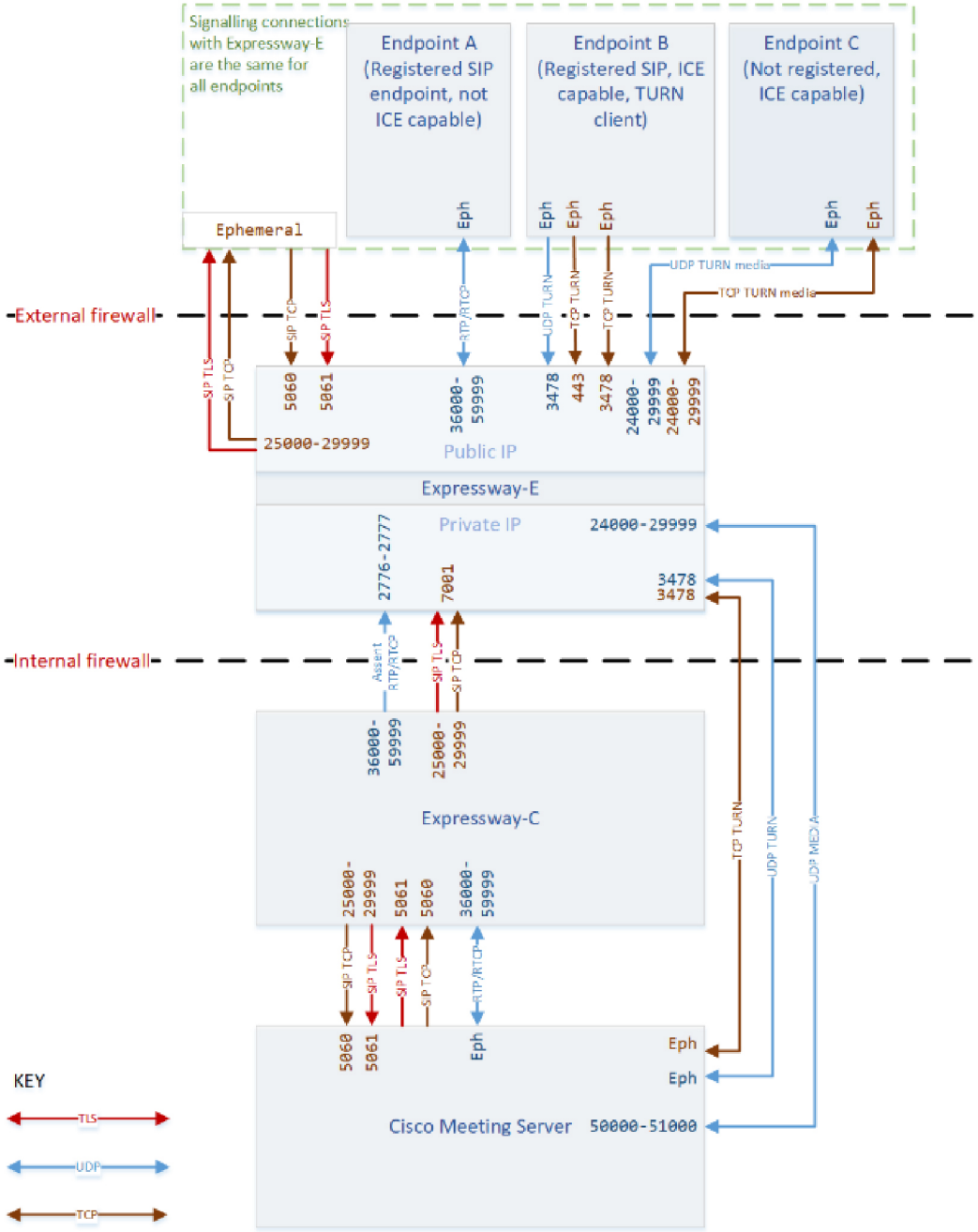
[11] バージョン X8.10 では、Expressway は、Cisco ミーティング WebRTC アプリケーションからのシグナリングを TCP 443 でリッスンすると同時に、TURN を TCP 443 でリッスンできません。Expressway は両方のトランスポートプロトコルに対して設定された TURN ポートでリッスンするため、TCP 3478 が表示されます。X8.11 以降、Expressway-E は TCP ポート 443 で TURN リクエストと Cisco Meeting Server リクエストの両方をリッスンできます。

[12] Expressway-E のパブリック IP アドレスの NAT リフレクションを許可するように外部ファイアウォールを設定する必要があります。（ファイアウォールは通常、同じ送信元と宛先の IP アドレスを持つパケットを信頼しません）。X12.5.3 リリースから、外部ファイアウォールで NAT リフレクションを設定する必要はありません。これは、Expressway には NAT リフレクションなしで自身のアドレスを検出する機能があるためです。

重要 X12.5.5 では、次の要件に従い、クラスタ化されたシステムに対してスタティック NAT 機能のサポートが拡張されます。ただし、TURN サーバーとして設定されているピアは、対応するパブリック インターフェイスのプライベート アドレスを使用して到達可能である必要があります。

[13] リレーポートが開いていない場合、Meeting Server は常に UDP ポート 3478 を使用してメディアをリレーします。これにより、CMA Web クライアントもリレーを使用している場合に、TURN サーバーの負荷が増加します。

Meeting Server 接続用 SIP エッジ（標準ベースのエンドポイント）



Cisco Meeting Server 用 SIP エッジポートリファレンス（標準ベースのエンドポイント）

表 *25 : Meeting Server* ポートリファレンス用 *SIP* エッジ

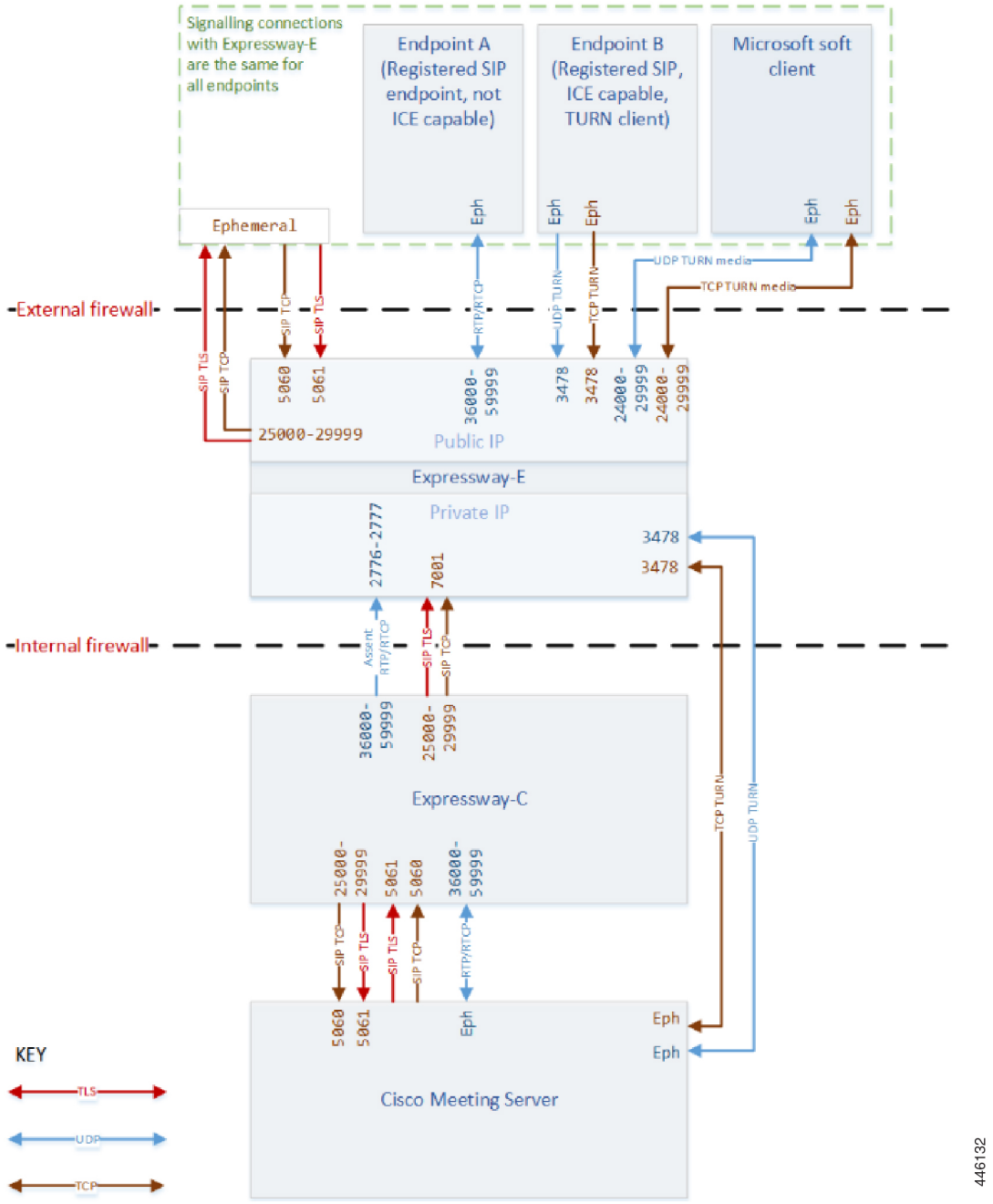
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP または TLS	Expressway-E	7001（最初のトラバーサルゾーンの場合。2 番目の場合は 7002 など）
SIP シグナリング	Expressway-C	5060	UDP	Meeting Server	[5060]
SIP シグナリング	Expressway-C	25000 ～ 29999	TLS	Meeting Server	5061
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	TCP	Expressway-E	[5060]
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	TLS	Expressway-E	5061
承認 RTP （トラバースされたメディア）	Expressway-C	36000 ～ 59999	UDP	Expressway-E	2776 または 36000（小規模/中規模） 36000 ～ 36010（偶数ポート）（大規模）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
承認 RTCP （トラバースされたメディア）	Expressway-C	36000 ～ 59999	UDP	Expressway-E	2777 または 36001（小規模/中規模） 36001 ～ 36011（奇数ポート）（大規模）
承認 RTP （トラバースされたメディア）	SIP エンドポイント（またはそのファイアウォール）	>=1024 エンドポイントポートではなく、メディアが出力されたファイアウォールポートである可能性があります	UDP	Expressway-E	36000 ～ 59999
承認 RTCP （トラバースされたメディア）	SIP エンドポイント（またはそのファイアウォール）	>=1024 エンドポイントポートではなく、メディアが出力されたファイアウォールポートである可能性があります	UDP	Expressway-E	36000 ～ 59999

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
承認 RTP （トラバースされたメディア）	Expressway-E	36000 ～ 59999	UDP	SIP エンドポイント（またはそのファイアウォール）	>=1024 Expressway はメディアを受信するまで待機し、その送信元ポート（エンドポイント ポートではなく、メディアがファイアウォールを出たポートである可能性があります）にメディアを送信します。
TURN リクエスト	任意の IP アドレス	>=1024（エンドポイントまたはファイアウォールからのシグナリングポート）	UDP & TCP	Expressway-E パブリック IP	3478（小規模/中規模） 3478 ～ 3483（大規模）
TURN リクエスト	Meeting Server	>=1024	UDP	Expressway-E プライベート IP	3478（小規模/中規模） 3478 ～ 3483（大規模）
TURN メディア	Expressway-E	24000 ～ 29999	UDP & TCP	任意の IP アドレス	>=1024

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN メディア	いずれか（Any）	>=1024 関連する ICE 候補のポート：ホスト IP ポート、サーバー再帰ポート（外部ファイアウォールポート）、または TURN サーバーポート	UDP & TCP	Expressway-E	24000 ～ 29999
TURN メディア	Meeting Server	50000 ～ 51000	UDP	Expressway-E プライベート IP	24000 ～ 29999

Meeting Server 接続用 SIP エッジ（Microsoft クライアント）



Cisco Meeting Server 用 SIP エッジポートリファレンス（Microsoft クライアント）

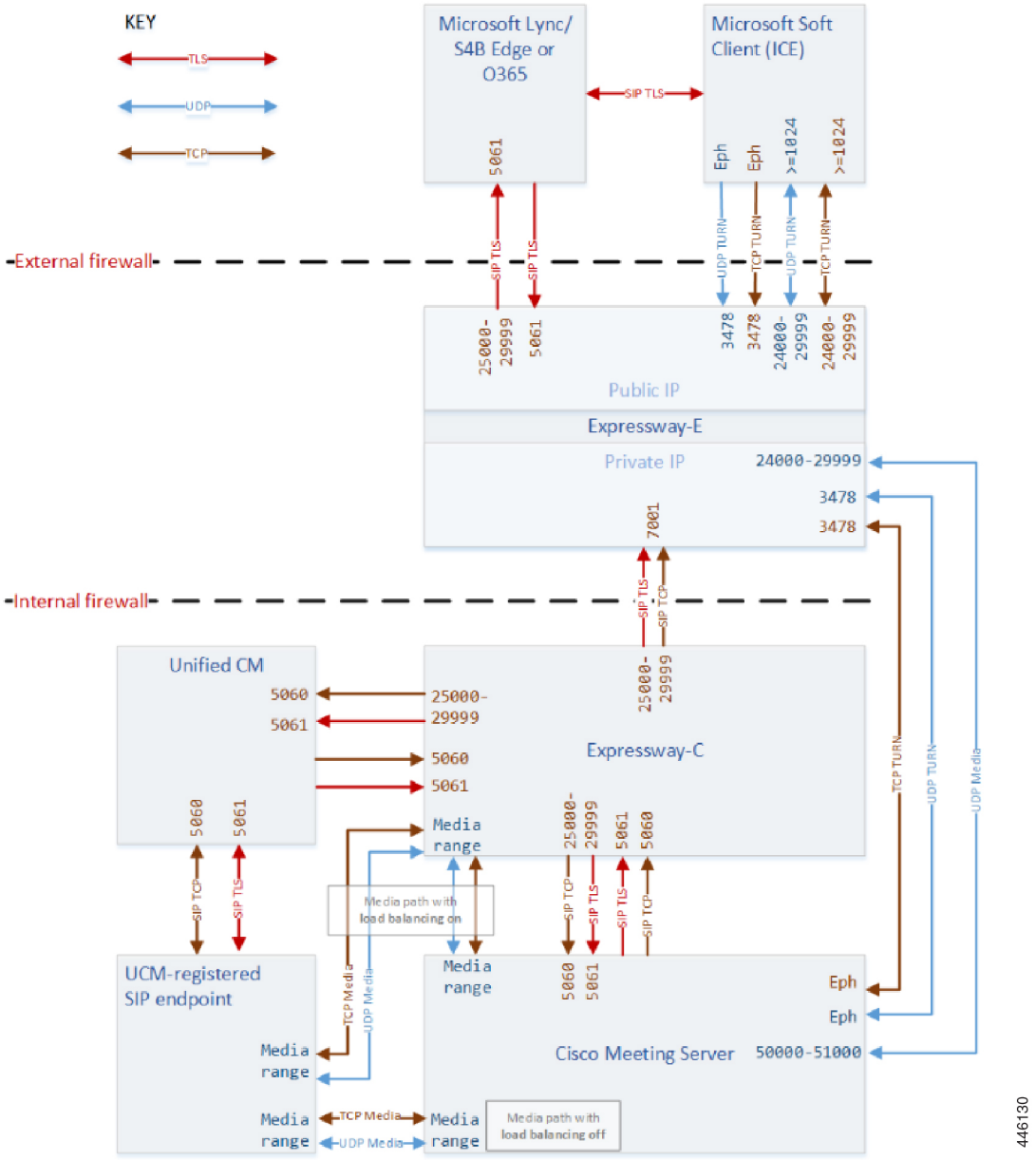
表 *26 : Meeting Server* ポートリファレンス用 *SIP* エッジ

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP または TLS	Expressway-E	7001（最初のトラバーサルゾーンの場合。2 番目の場合は 7002 など）
SIP シグナリング	Expressway-C	25000 ～ 29999	TLS	Meeting Server	5061
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	TCP	Expressway-E	[5060]
SIP シグナリング	SIP エンドポイント（またはそのファイアウォール）	>=1024	TLS	Expressway-E	5061
承認 RTP（トラバースされたメディア）	Expressway-C	36000 ～ 59999	UDP	Expressway-E	2776 または 36000（小規模/中規模） 36000 ～ 36010（偶数ポート）（大規模）
承認 RTCP（トラバースされたメディア）	Expressway-C	36000 ～ 59999	UDP	Expressway-E	2777 または 36001（小規模/中規模） 36001 ～ 36011（奇数ポート）（大規模）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
承認 RTP （トラバースされたメディア）	SIP エンドポイント（またはそのファイアウォール）	>=1024 エンドポイントポートではなく、メディアが出力されたファイアウォールポートである可能性があります	UDP	Expressway-E	36000 ～ 59999
承認 RTCP （トラバースされたメディア）	SIP エンドポイント（またはそのファイアウォール）	>=1024 エンドポイントポートではなく、メディアが出力されたファイアウォールポートである可能性があります	UDP	Expressway-E	36000 ～ 59999
承認 RTP （トラバースされたメディア）	Expressway-E	36000 ～ 59999	UDP	SIP エンドポイント（またはそのファイアウォール）	>=1024 Expressway はメディアを受信するまで待機し、その送信元ポート（エンドポイントポートではなく、メディアがファイアウォールを出たポートである可能性があります）にメディアを送信します。
TURN 制御	任意の IP アドレス	>=1024（エンドポイントまたはファイアウォールからのシグナリングポート）	UDP & TCP	Expressway-E	3478（小規模/中規模） 3478 ～ 3483（大規模）

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN メディア	Expressway-E	24000 ～ 29999	UDP & TCP	任意の IP アドレス	>=1024
TURN メディア	いずれか（Any）	>=1024 関連する ICE 候補のポート：ホスト IP ポート、サーバー再帰ポート（外部ファイアウォールポート）、または TURN サーバーポート	UDP & TCP	Expressway-E	24000 ～ 29999

接続マップ：Meeting Server を使用したポイントツーポイント Microsoft の相互運用性

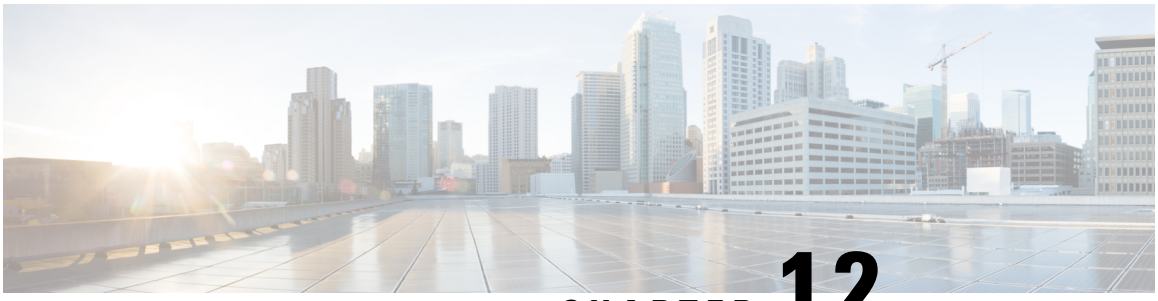


ポートリファレンス：Meeting Server を使用したポイントツーポイント Microsoft の相互運用性

表 *27 : Meeting Server* ポートリファレンスを使用したポイントツーポイント *Microsoft* 相互運用性

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP または TLS	Expressway-E	7001（最初のトラバーサルゾーンの場合。2 番目の場合は 7002 など）
SIP シグナリング	Expressway-C	25000 ～ 29999	TLS	Meeting Server	5061
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP	Meeting Server	[5060]
SIP シグナリング	Microsoft クライアントまたはそのファイアウォール	>=1024	TLS	Expressway-E	5061
SIP シグナリング	Expressway-C	25000 ～ 29999	TLS	Unified CM	5061
SIP シグナリング	Expressway-C	25000 ～ 29999	TCP	Unified CM	[5060]
SIP シグナリング	Unified CM	エフェメラル	TLS	Expressway-C	5061
SIP シグナリング	Unified CM	エフェメラル	TCP	Expressway-C	[5060]
TURN 制御	任意の IP アドレス	>=1024（エンドポイントまたはファイアウォールからのシグナリングポート）	UDP & TCP	Expressway-E	3478（小規模/中規模）

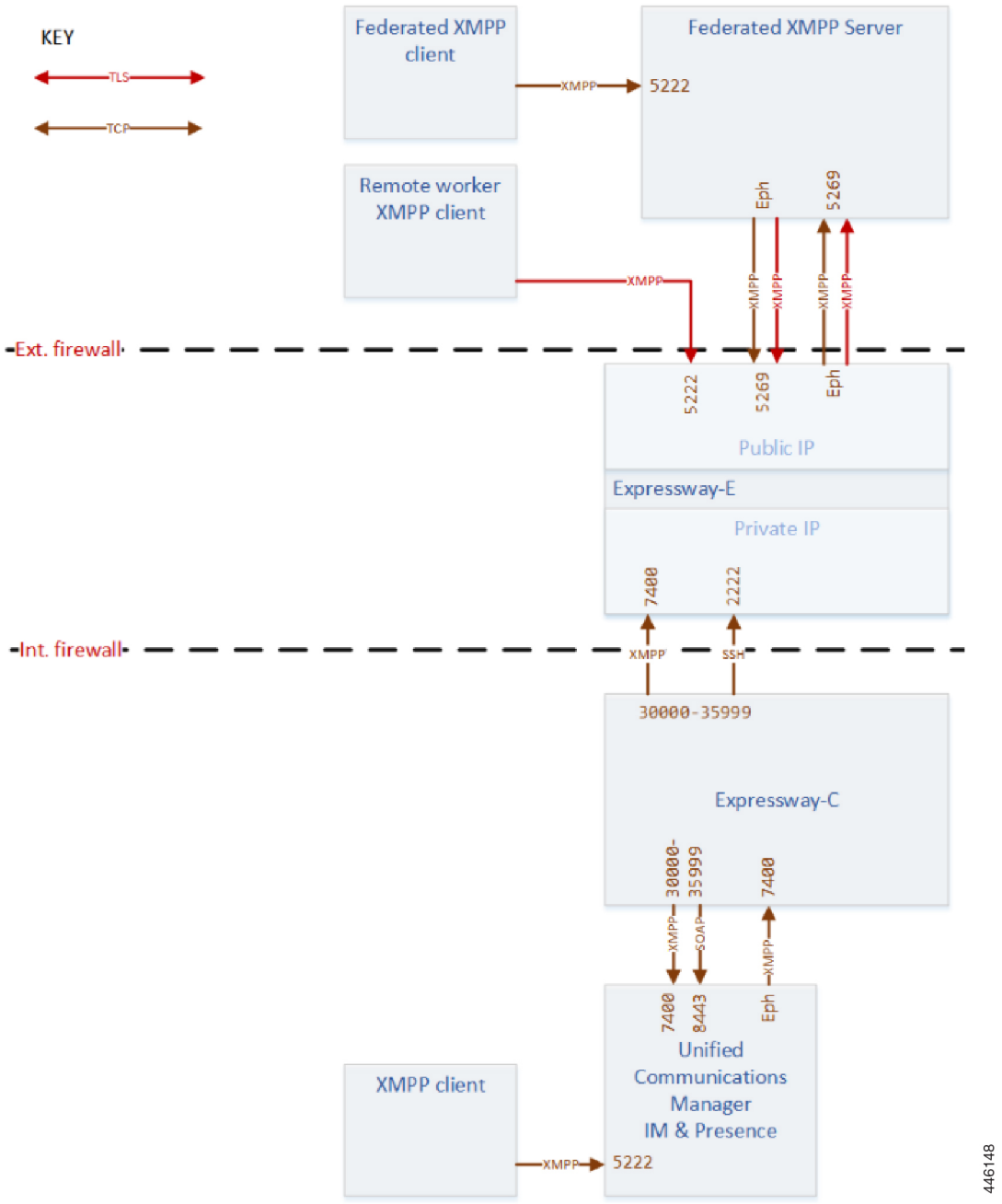
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
TURN リクエスト	Meeting Server	>=1024	UDP/TCP	Expressway-E プライベート IP	3478（小規模/中規模） 3478-3483（大規模）
TURN メディア	Expressway-E	24000 ～ 29999	UDP & TCP	任意の IP アドレス	>=1024
TURN メディア	いずれか（Any）	1024 以上の関連する ICE 候補のポート：ホスト IP ポート、サーバー再帰ポート（外部ファイアウォールポート）、または TURN サーバーポート	UDP & TCP	Expressway-E	24000 ～ 29999
TURN メディア	Meeting Server	50000 ～ 51000	UDP	Expressway-E プライベート IP	24000 ～ 29999



CHAPTER 12

XMPP フェデレーション

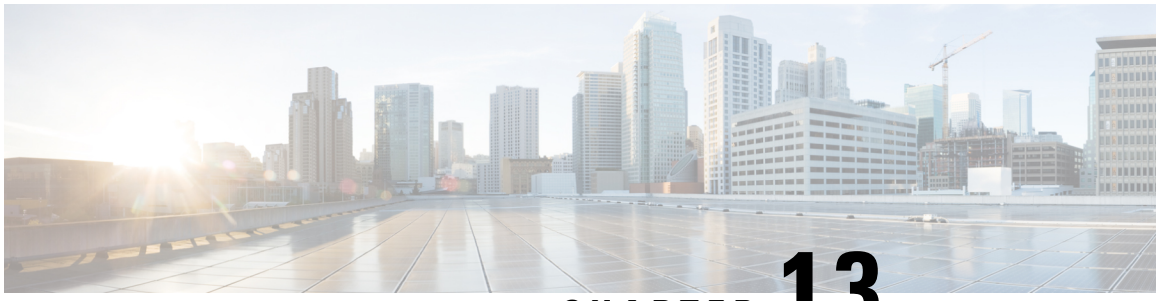
XMPP フェデレーション接続



XMPP ポートリファレンス

表 *28 : XMPP* フェデレーション ポート リファレンス

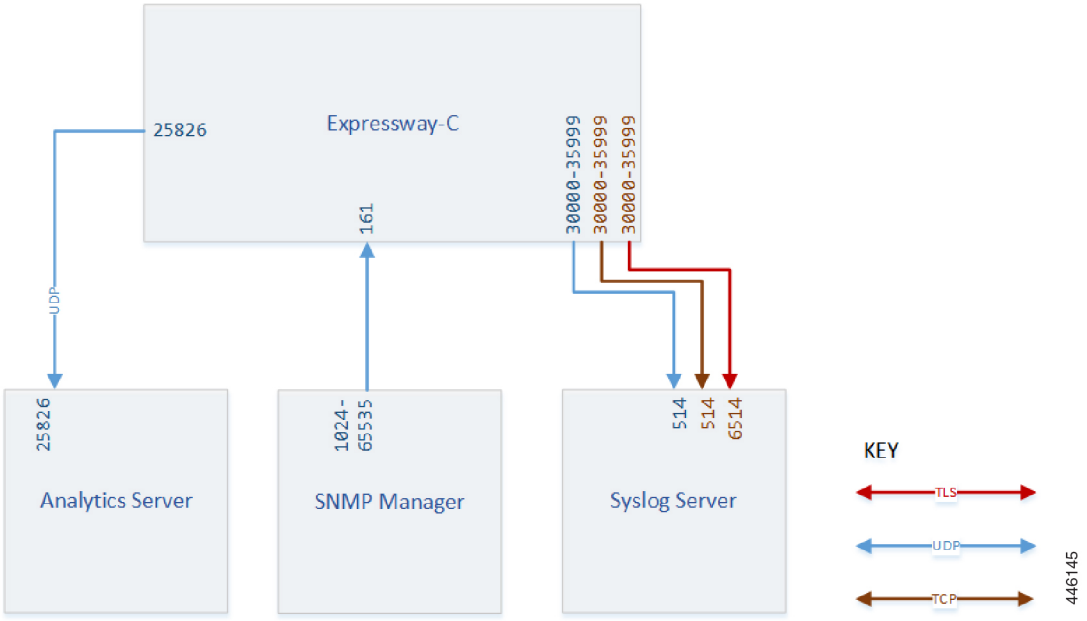
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
内部 XMPP 接続	Expressway-C	エフェメラル（30000 ～ 35999）	TCP	IM and Presence Service	7400
アウトバウンド XMPP トラバーサル	Expressway-C	エフェメラル（30000 ～ 35999）	TCP	Expressway-E	7400
フェデレーテッドドメインからのインバウンド XMPP 接続	任意（XMPP サーバー）	エフェメラル	TCP または TLS	Expressway-E	5269
フェデレーテッド ドメインへのアウトバウンド XMPP 接続	Expressway-E	エフェメラル（30000 ～ 35999）	TCP または TLS	任意（XMPP サーバー）	5269



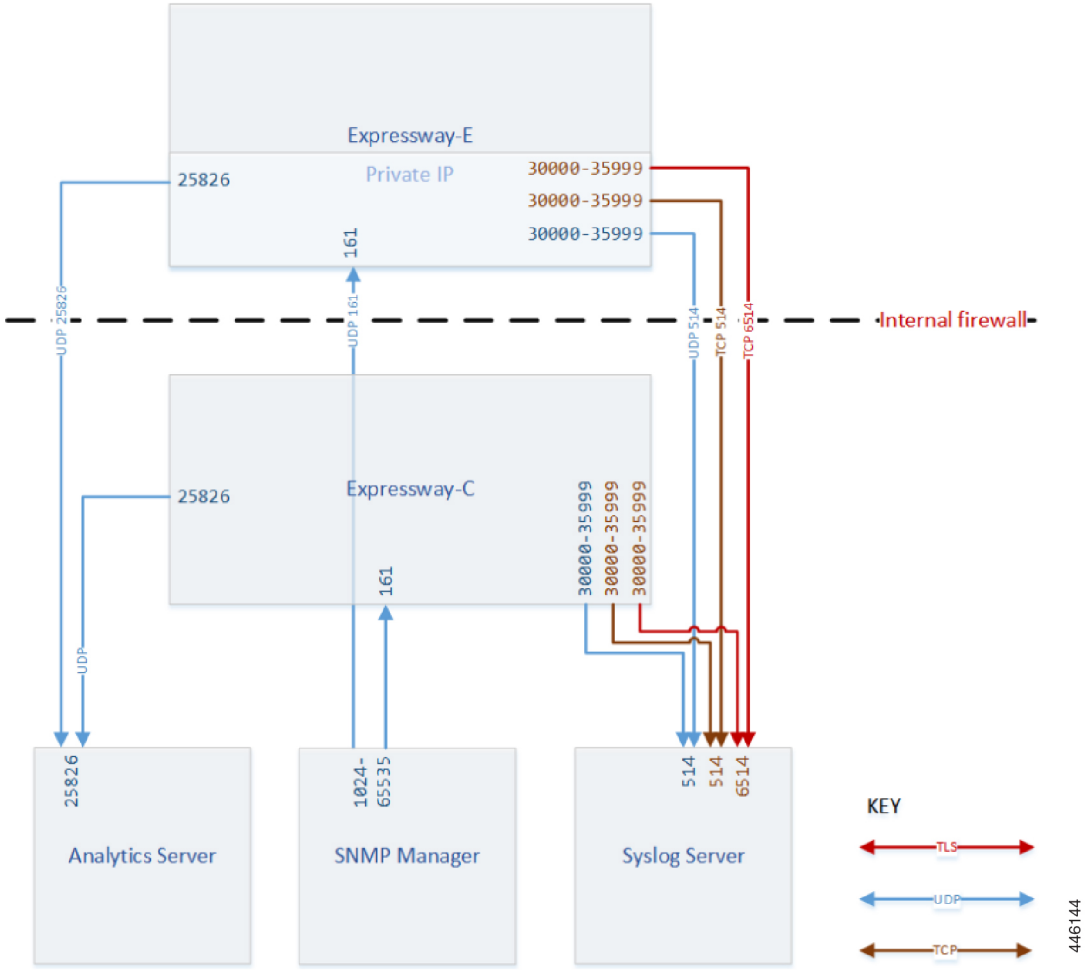
CHAPTER 13

サービスアビリティ

有用性：Expressway-C



有用性：トラバーサルペア

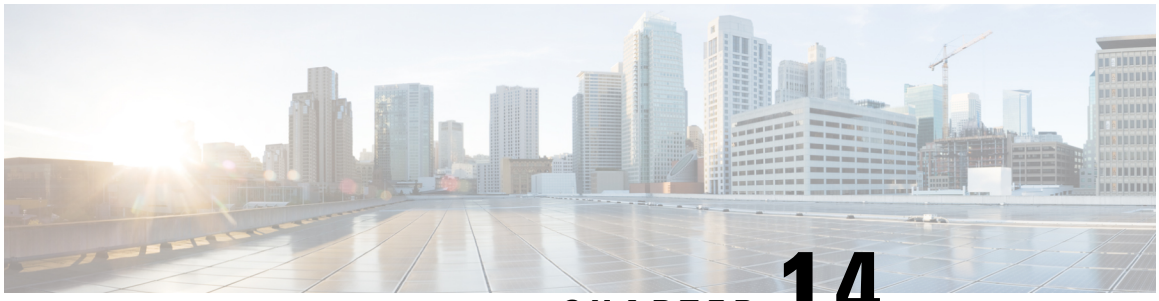


有用性ポート：トラバーサルペア

表 *29 : Expressway-E* および *Expressway-C* の有用性ポート

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
ネットワーク管理（SNMP）	SNMP マネージャ	1024 ～ 65535	UDP	Expressway-C	161
システムメトリック	Expressway	25826	UDP	分析サーバー	25826

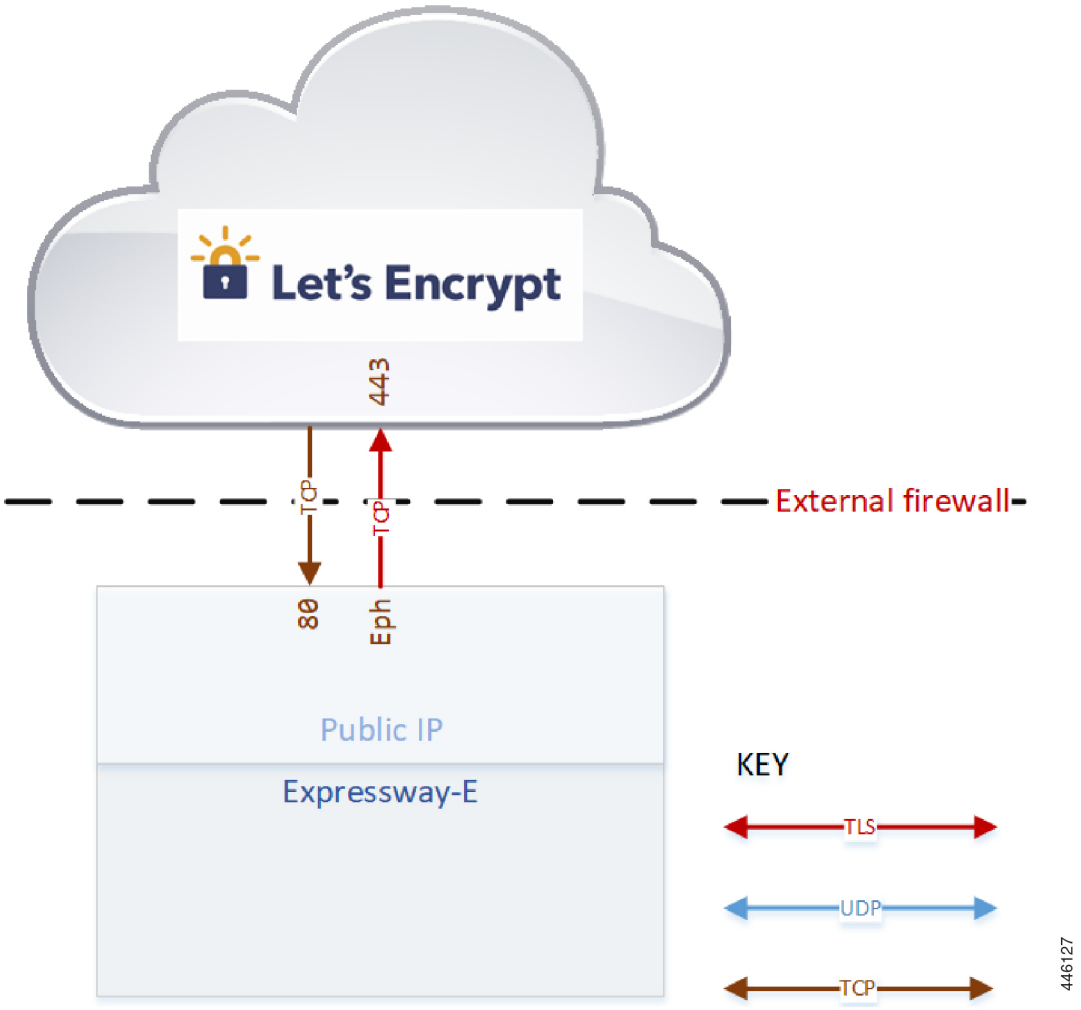
目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
リモートロギング（syslog）	Expressway	30000 ～ 35999	UDP	Syslog サーバー	514
リモートロギング（syslog）	Expressway	30000 ～ 35999	TCP	Syslog サーバー	514
リモートロギング（syslog）	Expressway	30000 ～ 35999	TLS	Syslog サーバー	6514



CHAPTER 14

ACME 証明書管理

ACME 証明書管理接続



Expressway-E ACME ポートリファレンス

表 *30 : Expressway-E* で *ACME (Automated Certificate Management Environment)* を導入するポートが必要

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
チャレンジファイルの書き込み	任意（ACME プロバイダーの IP アドレスは予測不能）	1024 ～ 65535	TCP	Expressway-E パブリック NIC	80

目的	送信元IP	送信元ポート	プロトコル	宛先IP	宛先ポート
証明書署名のリクエスト	Expressway-E パブリック NIC	エフェメラル	TLS	任意（ACME プロバイダードメイン）	443

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。