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。

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。