ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポートを備えた ALG—H.323 vTCP 機能により、H.323 アプリケーション レベル ゲートウェイ（ALG）が拡張され、単一 H.323 メッセージではない TCP セグメントをサポートします。仮想 TCP（vTCP）は TCP セグメント リアセンブルをサポートします。この機能の導入前は、H.323 ALG は TCP セグメントが完全な H.323 メッセージである場合にだけ TCP セグメントを処理していました。TCP セグメントに複数のメッセージが含まれていた場合は、H.323 ALG が TCP セグメントを無視し、そのパケットは処理されずに転送されていました。

このモジュールでは、ファイアウォールおよび NAT 対応のハイ アベイラビリティ（HA）サポートを備えた ALG—H.323 vTCP を設定する方法について説明します。

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP に関する制約事項

- 着信 TCP セグメントが完全な H.323 メッセージでない場合は、H.323 ALG がその TCP セグメントをバッファリングしメッセージの残りの部分を待機します。バッファリングされたデータは、ハイ アベイラビリティ（HA）用のスタンバイ デバイスに同期されません。
- vTCP がデータのバッファリングを開始した時点で、H.323 ALG のパフォーマンスに影響する可能性があります。

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP に関する情報

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを NAT が実行します。IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

基本 H.323 ALG サポート

H.323 は、パケットベース ネットワーク経由でのマルチメディア送信用の一連のネットワーク要素およびプロトコルを定義する ITU-T が公開している推奨事項です。H.323 は、マルチメディアの送信で使用されるさまざまなネットワーク要素を定義します。

現在、ほとんどの H.323 実装ではシグナリング用の転送メカニズムとして TCP が利用されていますが、H.323 バージョン 2 では基本 UDP トランスポートが有効になります。

- H.323 端末：この要素は、別の H.323 端末またはゲートウェイとの双方向通信を行うネットワークのエンドポイントです。
- H.323 ゲートウェイ：この要素は、H.323 端末と H.323 をサポートしないその他の端末との間のプロトコル変換を行います。
- H.323 ゲートキーパー：この要素は、アドレス変換、ネットワーク アクセス コントロール、帯域幅管理といったサービスを提供し、H.323 端末およびゲートウェイで構成されます。

次のコア プロトコルが H.323 仕様で規定されています。

- H.225：このプロトコルは、任意の 2 つの H.323 エンティティ間で通信を確立するために使用されるコール シグナリング方式を規定します。
- H.225 Registration, Admission, and Status（RAS）：このプロトコルは、アドレス解決およびアドミッション制御サービスのために、H.323 エンドポイントとゲートウェイによって使用されます。
- H.245：このプロトコルは、マルチメディア通信機能の交換と、オーディオ、ビデオ、およびデータ用の論理チャネルの開閉のために使用されます。

H.323 仕様では上記のプロトコルの他に、さまざまな IETF プロトコル（Real-time Transport Protocol（RTP）プロトコルや、オーディオ（G.711、G.729 など）およびビデオ（H.261、H.263、および H.264）コーデックなど）の使用についても規定しています。

NAT では、パケット ペイロード内の埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の取得といった、レイヤ 7 プロトコル固有のサービスを処理するために、さまざまな ALG を必要とします。H.323 ALG は、H.323 メッセージに対してこれらの特定サービスを実行します。

vTCP for ALG サポートの概要

レイヤ 7 プロトコルが TCP を使用してデータ転送を行う際は、アプリケーションの設計、最大セグメント サイズ（MSS）、TCP ウィンドウ サイズなどのさまざまな理由によって TCP ペイロードがセグメント化される場合があります。ファイアウォールと NAT がサポートするアプリケーション レベル ゲートウェイ（ALG）には、パケット インスペクションで TCP フラグメントを認識する機能がありません。vTCP が、ALG を使用して TCP セグメントを認識し、TCP ペイロードを解析する汎用フレームワークになります。

vTCP は、組み込みデータを書き直すために TCP ペイロード全体を必要とする NAT や Session Initiation Protocol（SIP）などのアプリケーションに役立ちます。ファイアウォールでは vTCP を使用して、ALG がパケット間でのデータ分割をサポートできるようにします。

ファイアウォールまたは NAT ALG を設定すると、vTCP 機能が有効になります。

vTCP は、現在のところ、Real Time Streaming Protocol（RTSP）および DNS ALG をサポートしています。

TCP 確認応答と確実な送信

vTCP は 2 つの TCP ホストの間に存在するため、TCP セグメントをもう一方のホストに送信する前に一時的に保存するためのバッファ スペースが必要です。vTCP はホスト間の適切なデータ伝送を保証します。vTCP は伝送するデータがさらに必要な場合は、送信側ホストに TCP 確認応答（ACK）を送信します。また、TCP フローの最初から受信側ホストが送信する ACK をトラッキングして、確認応答されたデータを詳細にモニタします。

vTCP は、TCP セグメントを再構成します。着信セグメントの IP ヘッダーおよび TCP ヘッダー情報は、確実に送信されるように vTCP バッファに保存されます。

NAT 対応アプリケーションの場合、vTCP は発信セグメントの長さにマイナーな変更を加えることができます。vTCP は最後のセグメントのデータ長を大きくするか、新しいセグメントを作成して、追加のデータを伝送することができます。新しく作成されたセグメントの IP ヘッダーまたは TCP ヘッダーは、オリジナルの着信セグメントから派生したものです。IP ヘッダーの合計の長さと TCP ヘッダーのシーケンス番号は、必要に応じて調整されます。

NAT ALG とファイアウォール ALG を使用した vTCP

ALG は、NAT およびファイアウォールのサブコンポーネントです。NAT とファイアウォールのいずれにも、ダイナミックに ALG を連結させるためのフレームワークがあります。ファイアウォールがレイヤ 7 インスペクションを実行する場合または NAT がレイヤ 7 フィックスアップを実行する場合は、ALG によって登録されたパーサー機能が呼び出され、ALG がパケット インスペクションを引き継ぎます。vTCP は、NAT またはファイアウォールとこれらのアプリケーションを使用する ALG を仲介します。つまり、パケットは、まず、vTCP で処理されてから、ALG に渡されます。vTCP は、TCP 接続内の両方向で TCP セグメントを再構築します。

ALG の概要：高可用性をサポートする H.323 vTCP

ファイアウォールおよび NAT の高可用性をサポートする ALG/H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするように H.323 アプリケーション レベル ゲートウェイ（ALG）を拡張します。H.323 ALG が vTCP と結合されると、ファイアウォールと NAT は vTCP を使用して H.323 ALG と対話するようになります。vTCP ではバッファ内のデータをスタンバイ デバイスに同期できないため、vTCP がデータのバッファリングを開始すると高可用性（HA）機能が影響を受けます。vTCP がデータをバッファリングしているときにスタンバイ デバイスへのスイッチオーバーが発生すると、バッファ内のデータがスタンバイ デバイスに同期されていないために接続がリセットされる可能性があります。vTCP がバッファ内のデータを確認応答した後は、そのデータは失われ、接続がリセットされます。ファイア

ウォールと NAT は HA を確保するためにスタンバイ デバイスにデータを同期しますが、vTCP がスタンバイ デバイスに同期するのは現在の接続のステータスだけなので、エラーが発生すると接続がリセットされます。

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP の設定方法

ALG の設定：ファイアウォール用のハイ アベイラビリティ サポートを備えた H.323 vTCP

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **inspect**
10. **exit**
11. **class class-default**
12. **exit**
13. **zone security** *zone-name*
14. **exit**
15. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
16. **service-policy type inspect** *policy-map-name*
17. **exit**
18. **interface** *type number*
19. **zone member security** *zone-name*
20. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any h.323-class`	検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol h323`	指定されたプロトコルを基づいて、クラス マップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol h323ras`	指定されたプロトコルを基づいて、クラス マップの一致基準を設定します。
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect h.323-policy`	検査タイプ ポリシー マップを作成し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 8	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect h.323-class`	アクションを実行するクラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 11	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシー マップ設定を、事前に定義したデフォルト クラスに適用します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config)# exit`	QoS ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone security** *zone-name* 例： `Device(config)# zone security inside`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ゾーン ペアを作成するには2つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が設定に含まれる必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 14	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security inside-outside source inside destination outside`	セキュリティ ゾーンのペアを作成して、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 16	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect h.323-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 17	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 18	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**zone member security** *zone-name* 例： `Device(config-if)# zone member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 20	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポートを備えた ALG—H.323 vTCP の設定例

例：ファイアウォールに対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP の設定

```
Device# configure terminal
Device(config)# class-map type inspect h.323-class
Device(config-cmap)# match protocol h323
Device(config-cmap)# match protocol h323ras
Device(config-cmap)# exit
Device(config)# policy-map type inspect h323-policy
Device(config-pmap)# class type inspect h323
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone-pair security inside-outside source inside destination outside
Device(config-sec-zone-pair)# service-policy type inspect h.323-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/1
```

```
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# zone-member security outside
Device(config-if)# end
```

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポートを備えた ALG-H.323 vTCP に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
ファイアウォール コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Services Command Reference』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1* : ファイアウォールと *NAT* に対するハイ アベイラビリティ サポートを使用した *ALG - H.323 vTCP* に関する機能情報

機能名	リリース	機能情報
ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP	Cisco IOS XE リリース 3.7S	ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするように H.323 ALG を拡張します。vTCP はセグメントの再構成をサポートします。この機能が導入される前は、H.323 メッセージが完全な場合にのみ、H.323 ALG が TCP セグメントを処理していました。TCP セグメントに複数のメッセージが含まれていた場合は、H.323 ALG が TCP セグメントを無視し、そのパケットは処理されずに転送されていました。

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。