ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた 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 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。 仮想 TCP（vTCP）は TCP セグメントの再構成をサポートします。 この機能の導入前は、H.323 ALG では、完全な H.323 メッセージである TCP セグメントのみを処理していました。 TCP セグメントが複数のメッセージである場合、H.323 ALG では TCP セグメントを無視し、パケットは処理されずに渡されていました。

このモジュールでは、ファイアウォールに対するハイ アベイラビリティ（HA）サポートを備えた ALG - H.323 vTCP の設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

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。

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の制約事項

- 着信 TCP セグメントが完全な H.323 メッセージではない場合、H.323 ALG ではメッセージの残りを待機中に TCP セグメントをバッファします。 バッファされたデータは、ハイ アベイラビリティ（HA）を得るためにスタンバイ デバイスに同期されません。
- vTCP によるデータのバッファ開始時に、H.323 ALG のパフォーマンスが影響を受ける可能性があります。

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP について

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、アプリケーション層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層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 の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。

- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能な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、NAT は、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 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 ネットワーク経由のマルチメディア送信用に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ネットワーク要素数を定義します。

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 を利用していますが、H.323 バージョン 2 では基本 UDP トランスポートがイネーブルにされます。

- 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提供する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 をサポートしない他の端末との間のプロトコル変換を提供します。
- 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 シグナリング方法について規定しています。
- H.225 登録、アドミッション、およびステータス（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用に、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、およびオーディオ、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。

示されているプロトコルに加え、H.323 仕様では、リアルタイム トランスポート（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）コーデックなどのさまざまな IETF プロトコル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、これら特定のサービスを実行します。

vTCP for ALG サポートの概要

レイヤ 7 プロトコルは TCP を使用してデータ転送を行い、TCP ペイロードはアプリケーション設計、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りセグメント化が可能です。 ファイアウォールおよび NAT でサポートされる ALG には、パケット インスペクションのために TCP フラグメントを認識する機能がありません。 vTCP は、TCP セグメントを理解し、TCP ペイロードを解析するために ALG で使用される汎用フレームワークです。

vTCP は、TCP ペイロード全体で埋め込みデータを書き直す必要がある NAT およびセッション開始プロトコル（SIP）などのアプリケーションで役立ちます。 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。

ファイアウォールおよび NAT ALG を設定すると、vTCP 機能がアクティブ化されます。

TCP 確認応答と確実な送信

vTCP は 2 つの TCP ホスト間に存在するため、TCP セグメントを他のホストに送信するまで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、データ伝送がホスト間で適切に行われるようにします。 vTCP では、データ伝送用にさらに多くのデータが必要な場合、送信ホストに TCP 確認応答（ACK）を送信します。 vTCP ではまた、受信ホストにより送信される ACK を TCP フローの始めから追跡し、確認応答データを注意深くモニタします。

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、確実な送信のために vTCP バッファに保存されます。

vTCP では、NAT 対応アプリケーションの発信セグメントの長さを細かく変更できます。 vTCP は最後のセグメントのデータ長を長くするか、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 コンテンツは、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。

vTCP と NAT およびファイアウォール ALG

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か、NAT がレイヤ 7 フィックスアップを実行すると、ALG により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 および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 との間を仲介します。 言い換えると、パケットはまず vTCP によって処理されてから、ALG に渡されます。 vTCP は、TCP 接続内で両方向の TCP セグメントを再構成します。

ハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の概要

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた 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 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 と組み合わせられると、ファイアウォールおよび NAT は vTCP を介して H.323 ALG と対話します。 vTCP がデータのバッファを開始すると、ハイ アベイラビリティ（HA）機能が影響を受けます。これは、vTCP ではバッファされたデータをスタンバイ デバイスに同期できないためです。 vTCP によるデータのバッファ中にスタンバイ デバイスへのスイッチオーバーが発生した場合、バッファされたデータがスタンバイ デバイスに同期されていないと、接続がリセットされることがあります。バッファされたデータが vTCP により確認されると、それらのデータは失われ、接続がリセットされます。 ファイアウォールおよび NAT は HA のためにデータを同期します。 vTCP はスタンバイ デバイスへの現在の接続状態のみを同期し、エラーが発生すると、接続がリセットされます。

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定方法

NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nat inside**
5. **exit**
6. **interface** *type number*
7. **ip nat outside**
8. **exit**
9. **ip nat pool** *pool-name start-ip end-ip* **prefix-length** *prefix-length*
10. **ip nat inside source list pool** *pool-name*
11. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
12. **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	**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。
ステップ 4	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されることを示します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	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、グローバル コンフィギュレーション モードに入ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	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。
ステップ 7	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されることを示します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	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、グローバル コンフィギュレーション モードに入ります。
ステップ 9	**ip nat pool** *pool-name start-ip end-ip* **prefix-length** *prefix-length* 例： `Device(config)# ip nat pool pool1 10.1.1.10 10.1.1.100 prefix-length 24`	NAT で使用される IP アドレス プールを定義します。
ステップ 10	**ip nat inside source list pool** *pool-name* 例： `Device(config)# ip nat inside source list pool pool1`	内部送信元アドレスの NAT をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 1 permit 10.0.0.0 255.255.255.0`	標準 IP アクセス リストを定義し、条件に合致している場合にパケットへのアクセスを許可します。
ステップ 12	**end** 例： `Device(config)# end`	グローバル 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。

次に、**show ip nat statistics** コマンドの出力例を示します。

```
Device# show ip nat statistics

Total active translations: 2 (0 static, 2 dynamic; 1 extended)
Outside interfaces:
  GigabitEthernet0/0/1
Inside interfaces:
  GigabitEthernet0/1/1
Hits: 0  Misses: 25
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 2
 pool pool1: netmask 255.255.255.0
        start 10.1.1.10 end 10.1.1.100
        type generic, total addresses 91, allocated 1 (1%), misses 0
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations

Pro  Inside global         Inside local          Outside local         Outside global
---  10.1.1.10             10.2.1.2              ---                   ---
udp  10.1.1.10:75          10.2.1.2:75           10.1.1.1:69           10.1.1.1:69
Total number of translations: 2
```

ファイアウォールおよびNATに対するハイ 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：NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# ip nat pool pool1 10.1.1.10 10.1.1.100 prefix-length 24
Device(config)# ip nat inside source list pool pool1
Device(config)# access-list 1 permit 10.0.0.0 255.255.255.0
Device(config)# end
```

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP に関するその他の関連資料

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
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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

ファイアウォールおよびNATに対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の機能情報

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*：ファイアウォールおよび *NAT* に対するハイ アベイラビリティ サポートを備えた *ALG - H.323 vTCP* の機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP	Cisco IOS XE Release 3.7S	ファイアウォールおよびNAT に対するハイ アベイラビリティ サポートを備えた 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 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。 この機能の導入前は、H.323 ALG では、完全な H.323 メッセージである TCP セグメントのみを処理していました。 TCP セグメントが複数のメッセージである場合、H.323 ALG では TCP セグメントを無視し、パケットは処理されずに渡されていました。

ファイアウォールおよび NAT に対するハイ アベイラビリティ サポートを備えた ALG - H.323 vTCP の機能情報