vTCP for ALG サポート

Virtual Transport Control Protocol（vTCP）機能は、Transport Control Protocol（TCP; 伝送制御プロトコル）セグメンテーションを適切に処理し、Cisco ファイアウォール、Network Address Translation（NAT; ネットワーク アドレス変換）、およびその他のアプリケーションでセグメントを解析するため、各種 Application Layer Gateway（ALG; アプリケーション層ゲートウェイ）プロトコル用のフレームワークを提供します。

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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「vTCP for ALG サポートに関する機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

vTCP for ALG サポートの前提条件

Cisco IOS XE Release 3.1 以降の Cisco IOS XE ソフトウェア リリースをシステムで実行している必要があります。最新版の NAT またはファイアウォール ALG を設定している必要があります。

vTCP for ALG サポートの制約事項

vTCP は、データ チャネル トラフィックをサポートしません。システム リソースを保護するため、vTCP は 8K を超えるメッセージの再構成をサポートしません。

vTCP は Hardware Availability（HA; ハードウェア アベイラビリティ）機能をサポートしません。HA は、主にファイアウォールまたは NAT に依存して、スタンバイ フォワーディング エンジンとのセッション情報を同期します。

サポートされる ALG

vTCP は、現在のところ、Real Time Streaming Protocol（RTSP; リアルタイム ストリーミング プロトコル）と Domain Name System（DNS; ドメイン ネーム システム）プロトコルをサポートしています。将来のリリースでは、Session Initiation Protocol（SIP）、H323、Skinny プロトコルに対する vTCP サポートが追加される予定です。

vTCP for ALG サポートについて

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、ペイロードは Maximum Segment Size（MSS; 最大セグメント サイズ）、アプリケーション設計、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。解析を実行するには、これらの TCP セグメントを適切に認識することが必要です。したがって、TCP セグメンテーションに対処するため、vTCP と呼ばれる汎用フレームワークがさまざまな ALG で使用されます。

SIP や NAT などの一部のアプリケーションでは、埋め込みデータを書き直すためにペイロード全体が必要になります。加えて、現在の ALG は、ファイアウォールで必要となるパケット間のデータ分割を考慮していません。そのため、vTCP は、現在の ALG に変更を加えずにファイアウォールに対処することが必要になります。NAT およびファイアウォール ALG コンフィギュレーションにより、vTCP 機能が有効になります。

TCP 確認応答と確実な送信

vTCP は 2 つの TCP ホストに存在するため、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。この処理中、vTCP はデータ送信がホスト間で適切に行われていることを保証します。これを行うため、vTCP は送信ホストに対して TCP 確認応答（ACK）を行います（さらにデータが必要な場合）。このプロセスとは別に、vTCP は TCP フローの始めから受信側ホストから送信される ACK を追跡し、確認応答された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 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発信セグメントの長さに変更が生じていないかをモニタできます。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 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。

vTCP と NAT/ファイアウォールおよび ALG との関係

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。ファイアウォールで L7 インスペクションが実行されると、または NAT で L7 フィックスアップが実行されると、ALG によって登録された解析機能が呼び出され、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 との間に介入します。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。

vTCP for ALG サポートの設定方法

RTSP、DNS、NAT、およびファイアウォール コンフィギュレーションでは、デフォルトで vTCP 機能が有効になります。そのため、vTCP 機能を有効にするための新しいコンフィギュレーションは必要ありません。

- 「Cisco ASR 1000 シリーズ ルータで RTSP をイネーブルにして vTCP を有効化」（P.3）

Cisco ASR 1000 シリーズ ルータで RTSP をイネーブルにして vTCP を有効化

RTSP パケット インスペクションを有効にするには、次の作業を実行します。

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. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **class class-default**
10. **exit**
11. **exit**
12. **zone security** *zone-name1*
13. **exit**

14. **zone security** *zone-name2*
15. **exit**
16. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
17. **service-policy type inspect** *policy-map-name*
18. **exit**
19. **interface** *type number*
20. **zone-member security** *zone-name1*
21. **exit**
22. **interface** *type number*
23. **zone-member security** *zone-name2*
24. **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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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： `Router(config)# class-map type inspect match-any rtsp_class1`	検査タイプ クラス マップを作成し、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： `Router(config-cmap)# match protocol rtsp`	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。 • RTSP の代わりに DNS を使用して、match protocol として DNS を設定します。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect rtsp_policy`	検査タイプ ポリシー マップを作成し、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 7	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect rtsp_class1`	アクションを実行するクラスを指定し、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。

	コマンドまたはアクション	目的
ステップ 8	**inspect** **例：** `Router(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 9	**class class-default** **例：** `Router(config-pmap-c)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。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。
ステップ 10	**exit** **例：** `Router(config-pmap-c)# exit`	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 11	**exit** **例：** `Router(config-pmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**zone security** *zone-name1* **例：** `Router(config)# zone security private`	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。
ステップ 13	**exit** **例：** `Router(config-sec-zone)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**zone security** *zone-name2* **例：** `Router(config)# zone security public`	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。
ステップ 15	**exit** **例：** `Router(config-sec-zone)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name* **例：** `Router(config)# zone-pair security pair-two source private destination public`	セキュリティ ゾーンのペアを作成し、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。 • 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 17	**service-policy type inspect** *policy-map-name* **例：** `Router(config-sec-zone-pair)# service-policy rtsp_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 18	**exit** **例：** `Router(config-sec-zone-pair)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 19	**interface** *type number* **例：** `Router(config)# GigabitEthernet0/1/0`	設定するインターフェイスを指定します。 • 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 20	**zone-member security** *zone-name1* **例：** `Router(config-if)# zone-member security private`	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 21	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 22	**interface** *type number* **例：** `Router(config)# GigabitEthernet0/1/0`	設定するインターフェイスを指定します。 • 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 23	**zone-member security** *zone-name* **例：** `Router(config-if)# zone-member security public`	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 24	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

トラブルシューティングのヒント

RTSP 対応のコンフィギュレーションの問題を解決するには、次のコマンドを使用できます。

- **clear zone-pair**
- **show policy-map type inspect zone-pair**
- **show zone-pair security**

vTCP for ALG サポートの設定例

ここでは、次の設定例について説明します。

例：Cisco ASR 1000 シリーズ ルータでの RTSP コンフィギュレーション

次に、RTSP インスペクションをイネーブルにするように Cisco ASR 1000 シリーズ ルータを設定する例を示します。

```
class-map type inspect match-any rtsp_class1
match protocol rtsp

policy-map type inspect rtsp_policy
class type inspect rtsp_class1
inspect
class class-default

zone security private
zone security public

zone-pair security pair-two source private destination public
service-policy type inspect rtsp_policy

interface GigabitEthernet0/1/0
 ip address 10.0.0.1 255.0.0.0
zone-member security private
!
interface GigabitEthernet0/1/1
 ip address 10.0.1.1 255.0.0.0
  zone-member security public
```

その他の関連資料

関連マニュアル

内容	参照先
Cisco IOS XE ファイアウォール コマンド	『*Cisco IOS Security Command Reference*』
Cisco ファイアウォール SIP 拡張機能：ALG	『*Cisco IOS XE Security Configuration Guide: Securing the Data Plane*』
ネットワーク アドレス変換	『*Cisco IOS XE IP Addressing Services Configuration*』

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 793	『*Transport Control Protocol*』
RFC 813	『*Window and Acknowledge Strategy in TCP*』

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

vTCP for ALG サポートに関する機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 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。

表 1　vTCP for ALG サポートに関する機能情報

機能名	リリース	機能情報
vTCP for ALG サポート	Cisco IOS XE Release 3.1S	この機能は、Cisco ASR 1000 シリーズ ルータ上で Cisco IOS XE ソフトウェアのファイアウォールおよび NAT ALG の TCP セグメンテーションおよび再構成を処理するための拡張機能を提供します。