Skinny Client Control Protocol のファイアウォール サポート

Skinny Client Control Protocol のファイアウォール サポート機能は、Cisco IOS XE ファイアウォールで VoIP と Skinny Client Control Protocol（SCCP）をサポートできるようにします。Cisco IP 電話は、SCCP を使用して Cisco Unified Communications Manager に接続および登録を行います。スケーラブルな環境で IP 電話と Cisco Unified Communications Manager 間の Cisco IOS XE ファイアウォールを設定できるようにするには、ファイアウォールが SCCP を検出して、メッセージ内で渡される情報を理解できる必要があります。Skinny Client Control Protocol のファイアウォール サポート機能によって、ファイアウォールは、Skinny クライアント（IP 電話など）と Cisco Unified Communications Manager 間で交換される Skinny コントロール パケットを検査し、Skinny データ チャネルがルータを通過できるようにルータを設定します。この機能は、ビデオ チャネルに対応するように SCCP のサポートを拡張します。

Skinny Client Control Protocol のファイアウォール サポートに関する前提条件

- システムは、Cisco IOS XE リリース 2.1 以降のリリースを実行している必要があります。
- SCCP アプリケーション レベル ゲートウェイ（ALG）が機能するためにはファイアウォールを有効にする必要があります。

- SCCP が機能するためには TFTP ALG を有効にする必要があります。これは、Skinny を使用する IP 電話には Cisco Unified Communications Manager からの TFTP コンフィギュレーション ファイルが必要なためです。

Skinny Client Control Protocol のファイアウォール サポートに関する制約事項

- IPv6 アドレスのインスペクションと変換はサポートされません。
- TCP セグメンテーションはサポートされません。

Skinny Client Control Protocol のファイアウォール サポートに関する情報

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。

SCCP インスペクションの概要

SCCP インスペクションでは、Cisco Unified Communications Manager を使用して、2 つの SCCP クライアント間での音声通信が可能です。Cisco Unified Communications Manager は TCP ポート 2000（デフォルトの SCCP ポート）を使用して、SCCP クライアントにサービスを提供します。初めに SCCP クライアントは TCP 接続を確立することでプライマリ Cisco Unified Communications Manager に接続し、その後、使用可能であればセカンダリ Cisco Unified Communications Manager に接続します。TCP 接続が確立された後、SCCP クライアントはプライマリ Cisco Unified Communications Manager に登録されます。プライマリ Cisco Unified Communications Manager はリブートするか、またはキープアライブ障害が発生するまで、制御 Cisco Unified Communications Manager として使用されます。したがって、SCCP クライアントと Cisco Unified Communications Manager 間の TCP 接続は永続的に存在し、クライアントとのコールを確立するために使用されます。TCP 接続が失敗すると、セカンダリ Cisco Unified Communications Manager が使用されます。最初の Cisco Unified Communications Manager と確立されたすべてのデータ チャネルは、コールの終了後に閉じられるまでアクティブのままです。

SCCP プロトコルは、ローカルで生成または終了した SCCP 制御チャネルを検査し、ファイアウォールを送信先または送信元とするメディア チャネルのピンホールを開閉します。ピンホールは、保護されたネットワークに対するアプリケーションで制御されたアクセスを可能するために、ファイアウォールを通じて開かれるポートです。

データ セッションの開閉に必要なメッセージのセットを下の表に示します。SCCP インスペクションは、アクセス リスト ピンホールを開閉するために使用されるデータ セッションを検査します。

表 *1 : SCCP* データ セッション メッセージ

Skinny インスペクション メッセージ	**説明**
CloseReceiveChannel	コールを中断する必要があることを示します。このメッセージが受信されると、ファイアウォールおよびNATにより作成されたすべての中間セッションはクリーンアップする必要があります。
OpenReceiveChannelACK	電話機が Cisco Unified Communications Manager から受信した OpenReceiveChannel メッセージを確認していることを示します。
StartMediaTransmission	コールの送信元または宛先である電話の Realtime Transport Protocol（RTP）情報が含まれます。メッセージには、IP アドレス、他方の電話がリッスンしている RTP ポート、およびコールを一意に識別するコール ID が含まれます。
StopMediaTransmission	通話が終了したことを表します。このメッセージを受信した後、セッションをクリーンアップすることができます。

Skinny インスペクション メッセージ	説明
StationCloseReceiveChannel	Skinny クライアント（このメッセージ中の情報に基づく）に受信チャネルを閉じるように指示します。
StationOpenMultiMediaReceiveChannelAck	このメッセージを送信する Skinny クライアントの IP アドレスおよびポート情報が含まれます。また、クライアントがビデオおよびデータ チャネルを受信する用意があるかどうかのステータスも含まれます。
StationOpenReceiveChannelAck	このメッセージを送信する Skinny クライアントの IP アドレスおよびポート情報が含まれます。このメッセージには、クライアントが音声トラフィックを受信する用意があるかどうかのステータスも含みます。
StationStartMediaTransmission	リモート Skinny クライアントの IP アドレスおよびポート情報を含みます。
StationStartMultiMediaTransmit	Cisco Unified Communications Manager がビデオまたはデータ チャネルの OpenLogicalChannelAck メッセージを受信したことを示します。
StationStopMediaTransmission	Skinny クライアント（このメッセージ中の情報に基づく）に音声トラフィックの送信を停止するように指示します。
StationStopSessionTransmission	Skinny クライアント（このメッセージ中の情報に基づく）に指定されたセッションを終了するように指示します。

ALG--SCCP バージョン 17 サポート

ALG - SCCP バージョン 17 サポート機能は、SCCP ALG で SCCP バージョン 17 パケットを解析できるようにします。Cisco Unified Communications Manager 7.0 および Cisco Unified Communications Manager 7.0 を使用する IP フォンでは、SCCP バージョン 17 のメッセージだけがサポートされています。IPv6 に対応するため、SCCP の形式はバージョン 17 から変更されました。SCCP ALG は、メッセージのプレフィックス内の SCCP バージョンをチェックしてから、バージョンに応じて解析します。SCCP メッセージのバージョンはメッセージヘッダーから抽出され、バージョンが 17 よりも大きい場合そのメッセージはバージョン 17 形式を使用して解析され、IPv4 アドレスおよびポート情報が抽出されます。SCCP ALG は、SCCP メッセージの IPv4 アドレス情報の検査および変換をサポートしています。

（注） IPv6 アドレスの検査および変換はサポートされていません。

次の SCCP ALG 処理メッセージの IP アドレス形式は、バージョン 17 で変更されました。

- StationOpenMultiMediaReceiveChannelAck
- StationOpenReceiveChannelAckMessage
- StationRegisterMessage
- StationStartMediaTransmissionAckMessage
- StationStartMultiMediaTransmissionAckMessage
- StationStartMediaTransmissionMessage
- StationStartMultiMediaTransmissionMessage

Skinny Client Control Protocol のファイアウォール サポートの設定方法

Skinny クラス マップとポリシー マップの設定

ファイアウォール設定で（**match protocol** コマンドを使用して）SCCP をイネーブルにする場合、（**match protocol** コマンドを使用して）TFTP をイネーブルにする必要があります。そうしないと、SCCP を使用する IP フォンは Cisco Unified Communications Manager と通信できません。SCCP は、Cisco Unified Communications Manager を使用して、2 つの Skinny クライアント間の音声通信を可能にします。

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. **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. **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：	特権 EXEC モードを有効にします。 • 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
	`Router> enable`	
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 cmap1`	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 skinny`	Skinny 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： `Router(config-cmap)# match protocol tftp`	TFTP クラス マップの一致基準を設定します。
ステップ 6	**exit** 例： `Router(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect pmap1`	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 8	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect cmap1`	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。
ステップ 9	**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 10	**exit** 例： `Router(config-pmap-c)# exit`	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： `Router(config-pmap)# 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。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-pmap)# end`	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、特権 EXEC モードを開始します。

ゾーン ペアの設定および SCCP ポリシー マップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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	**zone security** {*zone-name*	**default**} 例： `Router(config)# zone security zone1`	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。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(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 5	**zone security** {*zone-name* | **default**} 例： `Router(config)# zone security zone2`	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 6	**exit** 例： `Router(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 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Router(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） 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 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect pmap1`	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。 （注） 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 9	**exit** 例： `Router(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 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	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 11	**zone-member security** *zone-name* 例：	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。

	コマンドまたはアクション	目的
	`Router(config-if)# zone-member security zone1`	（注） 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）が、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 12	**exit** 例： `Router(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 13	**interface** *type number* 例： `Router(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 14	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security zone2`	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。
ステップ 15	**end** 例： `Router(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。

Skinny Control Protocol のファイアウォール サポートの設定例

例：SCCP クラス マップとポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any cmap1
Router(config-cmap)# match protocol skinny
Router(config-cmap)# match protocol tftp
Router(config-cmap)# exit
Router(config)# policy-map type inspect pmap1
Router(config-pmap)# class type inspect cmap1
```

```
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# end
```

例：ゾーン ペアの設定と SCCP ポリシー マップのアタッチ

```
Router# configure terminal
Router(config)# zone security zone1
Router(config-sec-zone)# exit
Router(config)# zone security zone2
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source zone1 destination zone2
Router(config-sec-zone-pair)# service-policy type inspect pmap1
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# zone-member security zone1
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/1/1
Router(config-if)# zone-member security zone2
Router(config-if)# end
```

Skinny Client Control Protocol のファイアウォール サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

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

Skinny Client Control Protocol のファイアウォール サポートに関する機能情報

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 *2 : Skinny Client Control Protocol* のファイアウォール サポートに関する機能情報

機能名	リリース	機能情報
ALG - SCCP V17 サポート	Cisco IOS XE リリース 3.5S	ALG - SCCP バージョン 17 サポート機能は、SCCP ALG で SCCP バージョン 17 パケットを解析できるようにします。SCCP 形式はバージョン 17 から IPv6 をサポートするように変更されました。

機能名	リリース	機能情報
ファイアウォール：SCCP ビデオ ALG サポート	Cisco IOS XE リリース 2.4	SCCP は、Cisco Unified Communications Manager を使用して、2 つの Skinny クライアント間の音声通信を可能にします。この機能は、Cisco ファイアウォールで、Skinny クライアントと Cisco Unified Communications Manager 間で交換される Skinny 制御パケットを検査できるようにします。 **match protocol** コマンドが変更されました。

機能名	リリース	機能情報
Skinny Client Control Protocol のファイアウォール サポート	Cisco IOS XE リリース 2.1	Skinny Client Control Protocol のファイアウォール サポート機能は、Cisco IOS XE ファイアウォールで VoIP と SCCP をサポートできるようにします。Cisco IP 電話は、SCCP を使用して Cisco Unified Communications Manager に接続および登録を行います。スケーラブルな環境で IP 電話と Cisco Unified Communications Manager 間の Cisco IOS XE ファイアウォールを設定できるようにするには、ファイアウォールが SCCP を検出して、メッセージ内で渡される情報を理解できる必要があります。Skinny Client Control Protocol のファイアウォール サポート機能によって、ファイアウォールは、Skinny クライアント（IP 電話など）と Cisco Unified Communications Manager 間で交換される Skinny コントロール パケットを検査し、Skinny データ チャネルがルータを通過できるようにルータを設定します。この機能は、ビデオ チャネルに対応するように SCCP のサポートを拡張します。

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。