ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化

ゾーンベース ポリシー ファイアウォールでは、アプリケーション レベル ゲートウェイ（ALG）およびアプリケーション インスペクションおよびコントロール（AIC）と、レイヤ 7 アプリケーション プロトコル インスペクションがサポートされています。レイヤ 7 アプリケーション プロトコル インスペクションを使用すると、セキュリティ モジュールを通過するプロトコルの動作の確認や、不要なトラフィックや悪意のあるトラフィックの識別が可能です。

ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能の導入前は、ALG/AIC 設定とともにレイヤ 7 プロトコル インスペクションが自動的に有効になりました。この機能を使用すると、**no application-inspect** コマンドを使用して、レイヤ 7 インスペクションを有効または無効にすることができます。

このモジュールでは、ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能について概説し、この機能を設定する方法について説明します。

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化に関する情報

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。

レイヤ7アプリケーション プロトコル インスペクションの有効化の概要

ゾーンベース ポリシー ファイアウォールでは、アプリケーション レベル ゲートウェイ（ALG）およびアプリケーション インスペクションおよびコントロール（AIC）と、レイヤ 7 プロトコル インスペクションがサポートされています。レイヤ 7 プロトコル インスペクションは ALG/AIC 設定とともに自動的に有効になります。

レイヤ 7 アプリケーション プロトコル インスペクションは、アプリケーション層プロトコルを解釈または理解し、適切なファイアウォールまたはネットワーク アドレス変換（NAT）アクションを実行する手法です。アプリケーションによっては、パケットがデバイスのセキュリティ モジュールを通過する際、パケットのデータ部分に特別な処理をする必要があります。レイヤ 7 アプリケーション プロトコル インスペクションを使用すると、セキュリティ モジュールを通過するプロトコルの動作の確認や、不要なトラフィックや悪意のあるトラフィックの識別が可能です。セキュリティ モジュールは、設定されているトラフィック ポリシーに基づい

てパケットの受け入れまたは拒否を行い、アプリケーションおよびサービスを安全に使用できるようにします。

アプリケーション インスペクションの実装の問題が原因で、アプリケーション パケットがドロップされることや、ネットワークが不安定になることがあります。ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能の導入前は、アプリケーション インスペクションを無効にするには、ターゲット レイヤ 7 プロトコル ポートを使用してアクセス コントロール リスト（ACL）を定義し、特定のレイヤ7プロトコルのインスペクションをバイパスするために、この ACL と、TCP または UDP プロトコルに一致するクラス マップを定義する必要がありました。

ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能が導入されたことで、**application-inspect** コマンドを使用して、特定のプロトコルまたはサポートされているすべてのレイヤ7プロトコルに対して、レイヤ7プロトコルインスペクションを有効または無効にできます。パラメータ マップの設定の変更は、新しいセッションにのみ適用されます。たとえば、FTP レイヤ 7 インスペクションを無効にすると、新規に作成されたセッションは FTP レイヤ7インスペクションをスキップしますが、この設定変更前にすでに確立されていた既存のセッションはFTP レイヤ7インスペクションを実行します。すべてのセッションで設定の変更を行う場合は、すべてのセッションを削除してから再作成する必要があります。

レイヤ 7 アプリケーション プロトコル インスペクションは、個々のパラメータ マップまたはグローバル ファイアウォールに対して有効にできます。

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化方法

ファイアウォールのレイヤ7アプリケーション プロトコル インスペクションの有効化

アプリケーション プロトコル インスペクションはデフォルトではイネーブルです。**no application-inspect** コマンドを使用して、アプリケーション プロトコル インスペクションを無効にします。

何らかの理由でアプリケーション プロトコル インスペクションを無効化した場合、**application-inspect** コマンドを使用して再設定します。**application-inspect** コマンドを設定する前に、**parameter-map type inspect** コマンドまたは **parameter-map type inspect-global** コマンドのいずれかを設定します。

いつでも **parameter-map type inspect** コマンドまたは **parameter-map type inspect-global** コマンドのいずれかのみを設定できます。

使用

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **parameter-map type inspect** *parameter-map-name*
   - **parameter-map type inspect-global**
4. **application-inspect** {**all** | *protocol-name*}
5. **exit**
6. **class-map type inspect** {**match-all** | **match-any**} *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** {*class-map-name* | **class-default**}
11. **inspect** *parameter-map-name*
12. **exit**
13. **class** {*class-map-name* | **class-default**}
14. **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： `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	次のいずれかを実行します。
	• **parameter-map type inspect** *parameter-map-name*
	• **parameter-map type inspect-global**
	例：
	`Device(config)# parameter-map type inspect pmap-fw`
	または
	`Device(config)# parameter-map type inspect-global`
		• （任意）接続しきい値、タイムアウト、およびその他の検査アクションに関連するパラメータに対して、ファイアウォールの検査タイプ パラメータ マップを有効にして、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• （任意）グローバル パラメータ マップを有効にし、パラメータ マップ タイプ検査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	**application-inspect** {**all**	*protocol-name*} 例： `Device(config-profile)# application-inspect msrpc`	指定されたプロトコルについてアプリケーション インスペクション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 5	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、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	**class-map type inspect** {**match-all** | **match-any**} *class-map-name* 例： `Device(config)# class-map type inspect match-any internet-traffic-class`	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 7	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol msrpc`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。
ステップ 8	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了して、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 9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect private-internet-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 10	**class type inspect** {*class-map-name* | **class-default**} 例： `Device(config-pmap)# class type inspect internet-traffic-class`	アクションを実行する対象のトラフィック 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 11	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap-fw`	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 12	**exit** 例： `Device(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 モードを終了して、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 13	**class** {*class-map-name* | **class-default**} 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 14	**end** 例： `Device(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 モードに戻ります。

レイヤ7アプリケーション プロトコル インスペクションを有効にするためのゾーンの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {**default** | *security-zone*}
4. **exit**
5. **zone security** {**default** | *security-zone*}
6. **exit**
7. **zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *security-zone*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *security-zone*
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： `Device> 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： `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	**zone security** {**default**	*security-zone*} 例： `Device(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。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 4	**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 モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {**default** | *security-zone*} 例： `Device(config)# zone security internet`	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： `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 モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private-internet source private destination internet`	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。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect private-internet-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 9	**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 モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(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** *security-zone* 例： `Device(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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。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。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/2/2`	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** *security-zone* 例： `Device(config-if)# zone-member security internet`	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： `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 モードに戻ります。

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化の設定例

例：ファイアウォールでのレイヤ7アプリケーション プロトコル インスペクションの有効化

次に、**parameter-map type inspect** コマンドを設定した後に、レイヤ 7 アプリケーション プロトコル インスペクションを有効にする例を示します。**parameter-map type inspect-global** コマンドを設定した後でも、アプリケーション インスペクションを有効にすることができます。

いつでも **parameter-map type inspect** コマンドまたは **parameter-map type inspect-global** コマンドのいずれかのみを設定できます。

```
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# application-inspect msrpc
Device(config-profile)# exit
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol msrpc
Device(config-cmap)# exit
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
Device(config-pmap-c)# exit
```

```
Device(config-pmap)# class class-default
Device(config-pmap)# end
```

例：レイヤ7アプリケーションプロトコルインスペクションを有効化するゾーンの設定

```
Device# configure terminal
Device(config)# zone security private
Device(config-sec-zone)# exit
Device(config)# zone security internet
Device(config-sec-zone)# exit
Device(config)# zone-pair security private-internet source private destination internet
Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# zone-member security private
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/2/2
Device(config-if)# zone-member security internet
Device(config-if)# end
```

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化に関する追加情報

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 Command List, All Releases』
ファイアウォール 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
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化に関する機能情報

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*: ゾーンベース ポリシー ファイアウォールでの *ALG* と *AIC* の有効化に関する機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化	Cisco IOS XE リリース 3.11S	ゾーンベース ポリシー ファイアウォールでは、アプリケーション レベル ゲートウェイ（ALG）およびアプリケーション インスペクションおよびコントロール（AIC）と、レイヤ 7 アプリケーション プロトコル インスペクションがサポートされています。レイヤ 7 アプリケーション プロトコル インスペクションは、プロトコル動作の確認と、セキュリティ モジュールを通過する不要なまたは悪意のあるトラフィックの識別を容易にします。 ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化機能が導入される前は、レイヤ 7 プロトコル インスペクションが ALG/AI C 設定とともに自動的に有効になりました。この機能を使用すると、no application-inspect コマンドを使用して、レイヤ 7 インスペクションを有効または無効にすることができます。 Cisco IOS XE リリース 3.11S では、この機能が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、Cisco 4400 シリーズ サービス統合型ルータ、およびシスコ クラウド サービス ルータ 1000V で導入されました。 次のコマンドが導入または変更されました。**application-inspect**、**show parameter-map type inspect**、および **show platform software firewall**。

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。