ゾーン不一致処理

ゾーン不一致処理機能を使用すれば、既存のセッションに関連付けられたゾーンペアを検証して、そのゾーンペアと一致するトラフィックをネットワークに転送することができます。セッションに関連付けられたゾーンペアを検証せずにネットワークへのトラフィックの転送を許可すると、セキュリティの脆弱性につながる可能性があります。

このモジュールでは、機能の概要とその設定方法について説明します。

ゾーン不一致処理に関する制約事項

zone-mismatch drop コマンドは、**parameter-map type inspect-vrf** コマンド、**parameter-map type inspect-zone** コマンド、および **parameter-map type inspect global** コマンドの下で設定できません。

ゾーン不一致処理に関する情報

ゾーン不一致処理の概要

ゾーンベース ファイアウォールは、送信元ゾーンから宛先ゾーンに流れるトラフィック用のセッションを作成し、そのトラフィックが宛先ゾーンから送信元ゾーンに戻るときに照合を行います。ゾーンとは、同様の機能を果たすインターフェイスのグループです。ゾーンペアを使用すれば、その一部である 2 つのセキュリティ ゾーン間の単方向ファイアウォール ポリシーを指定することができます。

トラフィックの最初のパケットに対して、ファイアウォールがパケットの入力インターフェイスと出力インターフェイスに関連付けられたゾーンペアをチェックし、パケットを検証してから、検査可能なトラフィック用のセッションを作成します。また、リターン トラフィックが戻ってきたら、ファイアウォールが最初のパケットに基づいてセッション ルックアップを実行し、既存のセッションを検索します。ファイアウォールが一致するセッションを見つけると、トラフィックの通過を許可し、リターン トラフィックに関連付けられたゾーンが既存のセッションに関連付けられたゾーンペアと一致するかどうかをチェックしません。セッションに関連付けられたゾーンペアを検証せずにネットワークへのトラフィックの転送を許可すると、セキュリティの脆弱性につながる可能性があります。

ゾーン不一致処理機能を使用すれば、既存のセッションに関連付けられたゾーンペアを検証して、そのゾーン ペアと一致するトラフィックをネットワークに転送することができます。**zone-mismatch drop** コマンドを設定する場合、ファイアウォールは、既存のセッションと一致するもののパケットが出入りするゾーンとゾーンペアが一致しないすべてのパケット（IPv4 と IPv6）をドロップします。この機能は、ハイ アベイラビリティおよび In-Service Software Upgrade（ISSU）と連動します。

parameter-map type inspect-global コマンドの下で **zone-mismatch drop** コマンドを設定する場合、ゾーン不一致処理の設定がグローバルファイアウォールの設定に適用されます。すべてのゾーン間のトラフィックでゾーン ペア不一致が検査されます。

parameter-map type inspect コマンドの下で **zone-mismatch drop** コマンドを設定することもできます。この場合は、ゾーン不一致処理機能をポリシー単位で適用することができます。

zone-mismatch drop コマンドを設定する場合、その設定は新しいセッションにのみ適用されます。既存のセッションでは、そのセッションが同じゾーンペアに属していなくても、トラフィックはドロップされません。

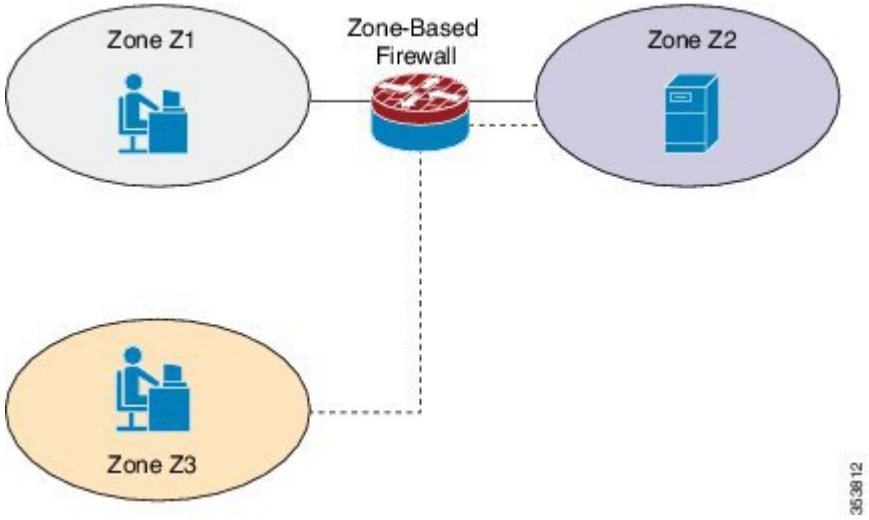
ゾーン不一致処理機能の導入シナリオ

ここでは、ゾーン不一致処理機能が導入される一般的なシナリオについて説明します。

ゾーンベース ファイアウォール アプリケーションによるトラフィック インスペクション

次の図は、ゾーン不一致処理機能が有効な場合のファイアウォールによるトラフィック インスペクションを示します。

図 *1:* ゾーンベース ファイアウォール アプリケーションによるトラフィック インスペクション



ゾーン Z1 と Z2 は同一のゾーンペアに含まれており、このゾーンペアには、**zone-mismatch drop** コマンドが設定されているパラメータマップがあります。ゾーン Z3 はゾーン ペアに含まれていないため、Z3 からのトラフィックは、インターフェイス 1 とインターフェイス 2 の間のファイアウォール セッションに一致する場合でも、ドロップされます。

ゾーン Z3 が追加されたゾーンペアに関連付けられているパラメータマップに対して **zone-mismatch drop** コマンドを設定すると、Z1 と Z2 の間で確立されるセッションに対しては、その設定は反映されません。ただし、**parameter-map type inspect-global** コマンドの下で **zone-mismatch drop** コマンドを設定すると、すべてのゾーン間のトラフィックに対してその設定が適用されます。

ゾーンベース ファイアウォールで設定されたアプリケーション レイヤ ゲートウェイ

一部のアプリケーション レイヤ ゲートウェイ（ALG）はアプリケーション レベル ゲートウェイとも呼ばれ、動作するには複数のコントロールおよびメディア チャネルが必要です。ゾーンベース ファイアウォールでは、制御チャネルおよびメディア チャネルが ALG の同一ゾーンペアに含まれることは義務付けられません。メディアチャネルまたはデータチャネルに対して **zone-mismatch drop** コマンドを設定する場合、この設定が有効になるのは、不明確なセッションから明確なセッションにメディアチャネルまたはデータチャネルが昇格した後です。ゾーンベースファイアウォールは、これらの明確なセッションを通常のセッションと同様にチェックします。不明確なセッションとは、5 タプル情報が含まれていないセッションです。

ゾーン不一致処理の設定方法

ゾーン不一致処理の設定

zone-mismatch drop コマンドは、**parameter-map type inspect-vrf**、**parameter-map type inspect-zone**、および **parameter-map type inspect global** コマンドの下で設定できません。

zone-mismatch drop コマンドを **parameter-map type inspect-global** コマンドの下で設定した場合、ゾーン不一致処理の設定はグローバルファイアウォール設定に適用されます。

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. **zone-mismatch drop**
5. **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`	ユーザ 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）。
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 pmap1`
	`or`
	`Device(config)# parameter-map type inspect-global`
		接続しきい値、タイムアウト、およびその他の inspect アクションに関連するパラメータの検査タイプ パラメータ マップを設定し、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	**zone-mismatch drop** 例： `Device(config-profile)# zone-mismatch drop`	既存のセッションに接続しているゾーン ペアを検証し、ゾーン ペアに一致するトラフィックをネットワークに対して許可します。着信セッションのゾーン ペアがセッションが到着または離脱するゾーンと一致しない場合、ファイアウォールはこれらのパケットをドロップします。
ステップ 5	**end** 例： `Device(config-profile)# end`	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、特権 EXEC モードに戻ります。

ゾーン不一致処理の設定例

例：ゾーン不一致処理の設定

次の例では、ゾーン不一致処理機能がパラメータ マップ pmap-fw に対して有効になっています。

```
! Configuring zones
Device(config)# zone security private
Device(config-sec-zone)# exit
Device(config)# zone security public
Device(config-sec-zone)# exit
Device(config)# zone security internet
Device(config-sec-zone)# exit

! Attaching zones to interfaces
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# zone-member security private
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# ip address 209.165.200.226 255.255.255.0
Device(config-if)# zone-member security public
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/1
Device(config-if)# ip address 198.51.100.1 255.255.255.0
Device(config-if)# zone-member security internet
Device(config-if)# no shutdown
Device(config-if)# exit

!Configuring the Zone Mismatch Handling feature
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# zone-mismatch drop
Device(config-profile)# exit

!Configuring class maps
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit

! Configuring policy maps and class matching
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-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit

! Configuring zone pairs
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)# end
```

ゾーン不一致処理に関する追加情報

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』
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
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

ゾーン不一致処理に関する機能情報

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* : ゾーン不一致処理に関する機能情報

機能名	リリース	機能情報
ゾーン不一致処理	Cisco IOS XE 3.15S	ゾーン不一致処理機能を使用すれば、既存のセッションに関連付けられたゾーン ペアを検証して、そのゾーンペアと一致するトラフィックをネットワークに転送することができます。 この機能は、Cisco 4400 シリーズ サービス統合型ルータ、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、およびシスコ クラウド サービス ルータ 1000V シリーズでサポートされます。 次のコマンドが導入されました：**zone-mismatch handling**

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。