ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプション

ゾーンベース ポリシー ファイアウォール機能の TCP ウィンドウ スケーリング オプションのルーズ チェックは、ファイアウォールでの TCP ウィンドウ スケーリング オプションの厳格なチェックを無効にします。

ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプションに関する情報

TCP ウィンドウ スケーリングのルーズ チェック オプションの概要

TCP は、高帯域幅および高速データ パスでのパフォーマンスを向上させる、さまざまな TCP 拡張機能を提供しています。このような拡張機能の 1 つが、TCP ウィンドウ スケーリング オプションです。TCP ウィンドウ スケーリングのルーズ チェック オプションは、RFC 1323 に記述されているウィンドウ スケーリング オプションの厳密なチェックを無効にします。

広帯域高遅延ネットワーク（LFN）と呼ばれる大きな帯域遅延積の特性を持つネットワーク経路での TCP のパフォーマンスを改善するため、より大きなウィンドウ サイズが推奨されます。

TCP ウィンドウ スケーリングにより、TCP ウィンドウの定義は 32 ビットに拡大され、スケール ファクタを使用して TCP ヘッダーの 16 ビット ウィンドウ フィールドでこの 32 ビットの値を伝送します。ウィンドウ サイズはスケール係数 14 まで大きくすることができます。典型的なアプリケーションは、広帯域高遅延ネットワークで動作するときにスケール係数 3 を使います。

ファイアウォールの実装により、TCP ウィンドウ スケーリング オプションの厳密なチェックが適用されます。この場合、ファイアウォールは、TCP スリーウェイ ハンドシェイクの初期同期（SYN）パケットで TCP ウィンドウ スケーリング オプションを受信しなかった場合、TCP ウィンドウ スケーリング オプションを使用する SYN/ACK パケットをドロップします。ウィンドウ スケーリング オプションは SYN ビットがオンに設定された SYN セグメントでのみ送信されます。したがって、接続のオープン時にウィンドウ スケールが各方向で固定されます。

tcp window-scale-enforcement loose コマンドを使用すると、TCP SYN セグメントでの TCP ウィンドウ スケーリング オプションの厳格なチェックが無効になります。

ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプションの設定方法

ファイアウォールの TCP ウィンドウ スケーリング オプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **tcp window-scale-enforcement loose**
5. **exit**
6. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
7. **match protocol** [*parameter-map*] [**signature**]
8. **exit**
9. **policy-map type inspect***policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect** [*parameter-map-name*]
12. **exit**
13. **class** *name*
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	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} 例： `Device(config)# parameter-map type inspect pmap-fw`	検査パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp window-scale-enforcement loose** 例： `Device(config-profile)# tcp window-scale-enforcement loose`	ファイアウォールでの TCP ウィンドウ スケーリング オプションの厳密なチェックを無効にします。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	プロファイル 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 6	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any internet-traffic-class`	検査タイプ クラス マップを作成して、QoS 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** [*parameter-map*] [**signature**] 例： `Device(config-cmap)# match protocol tcp`	指定され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`	QoS クラス マップ 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 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 マップを作成して、QoS 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。

	コマンドまたはアクション	目的
ステップ 10	**class type inspect** *class-map-name* 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`	QoS 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、QoS 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** *name* 例： `Device(config-pmap)# class class-default`	指定したデータリンク接続識別子（DLCI）にマップ クラスを関連付けます。
ステップ 14	**end** 例： `Device(config-pmap)# end`	QoS 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。

TCP ウィンドウ スケーリングのゾーンとゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address*
5. **zone-member security** *security-zone-name*
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address*
9. **zone-member security** *security-zone-name*
10. **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）。

	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 0/1/5`	インターフェイスを指定し、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 address** *ip-address* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイス IP アドレスを割り当てます。
ステップ 5	**zone-member security** *security-zone-name* 例： `Device(config-if)# zone-member security private`	インターフェイスをゾーン メンバーとして設定します。
ステップ 6	**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 7	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/6`	インターフェイスを指定し、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 8	**ip address** *ip-address* 例： `Device(config-if)# ip address 209.165.200.225 255.255.255.0`	IP アドレスをインターフェイスに割り当てます。
ステップ 9	**zone-member security** *security-zone-name* 例： `Device(config-if)# zone-member security internet`	インターフェイスをゾーン メンバーとして設定します。
ステップ 10	**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。

TCP ウィンドウ スケーリングの設定例

例：ファイアウォールの TCP ウィンドウ スケーリング オプションの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# tcp window-scale-enforcement loose
Device(config-profile)# exit
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol tcp
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：TCP ウィンドウ スケーリングのゾーンとゾーン ペアの設定

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# zone-member security private
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# ip address 209.165.200.225 255.255.255.0
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 TCP ウィンドウ スケーリングのルーズ チェック オプションに関する機能情報

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 *TCP* ウィンドウ スケーリングのルーズ チェック オプションに関する機能情報

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 TCP ウィンドウ スケーリングのルーズ チェック オプション	Cisco IOS XE リリース 3.10S	ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプション機能は、IOS-XE ファイアウォール内の TCP ウィンドウ スケーリング オプションの厳密なチェックを無効にします。 次のコマンドが導入または変更されました。**tcp window-scale-enforcement loose** Cisco IOS XE リリース 3.10S で、Cisco CSR 1000 シリーズルータのサポートが追加されました。

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。