ファイアウォール TCP SYN Cookie の設定

ファイアウォール TCP SYN Cookie 機能は、TCP SYN フラッディング攻撃からファイアウォールを保護します。TCP SYN フラッディング攻撃は、サービス妨害（DoS）攻撃の一種です。通常、TCP 同期（SYN）パケットは、ファイアウォールの背後にある対象のエンド ホストまたは一定範囲のサブネット アドレスに送信されます。これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。スプーフィング攻撃とは、個人またはプログラムが、データを改ざんして不正な優位性を獲得し、別のものになりすますことです。TCP SYN フラッディングは、ファイアウォールまたはエンドホスト上のすべてのリソースを占有し、そのために正当なトラフィックに対する DoS が発生します。ファイアウォールおよびファイアウォール背後のエンド ホストでの TCP SYN フラッディングを防ぐには、ファイアウォール TCP SYN Cookie 機能を設定する必要があります。

ファイアウォール TCP SYN Cookie の設定に関する制約事項

- デフォルトのゾーンはゾーン タイプのパラメータ マップをサポートしていないため、デフォルトのゾーンのファイアウォール TCP SYN Cookie 機能を設定することはできません。
- ファイアウォール TCP SYN Cookie 機能は、サブスクライバ単位のファイアウォールをサポートしていません。

ファイアウォール TCP SYN Cookie の設定について

TCP SYN フラッド攻撃

ファイアウォール TCP SYN Cookie 機能は、DoS 攻撃の一種である TCP SYN フラッディング攻撃からファイアウォールを保護するソフトウェアを実装します。

SYN フラッディング攻撃は、ハッカーがサーバに膨大な数の接続要求をフラッドすることによって発生します。これらのメッセージには到達不能の返信アドレスが含まれているため、接続を確立できません。未解決のオープン接続の数が増え、最終的にはサーバで処理しきれなくなり、有効な要求へのサービスが拒否されるようになるため、正当なユーザの Web サイトへの接続、電子メールのアクセス、FTP サービスの使用などが妨げられます。

SYN フラッド攻撃は、次の 2 つのタイプに分類されます。

- ホスト フラッド：SYN フラッド パケットが単一のホストに送信され、そのホスト上のすべてのリソースを使用することが意図されます。
- ファイアウォールセッションテーブルフラッド：SYNフラッドパケットはファイアウォールの背後のアドレスの範囲に送信され、ファイアウォール上のセッションテーブルリソースを枯渇させ、その結果、リソースの拒否がファイアウォールを通過するトラフィックを正当化することが意図されます。

ファイアウォール TCP SYN Cookie 機能は、TCP 接続要求を代行受信して検証することにより、SYNフラッディング攻撃を防止するのに役立ちます。ファイアウォールは、クライアントからサーバに送信される TCP SYN パケットを代行受信します。TCP SYN Cookie がトリガーされると、設定された VPN ルーティングおよび転送（VRF）またはゾーン宛てのすべての SYN パケットに作用します。TCP SYN Cookie は宛先サーバの代わりにクライアントとの接続を確立し、クライアントの代わりにサーバとの別の接続を確立して、2 つの半接続を透過的に結び付けます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。TCP SYN Cookie は接続されている間、パケットを代行受信および転送します。

ファイアウォール TCP SYN Cookie 機能は、グローバル ルーティング ドメインと VRF ドメインのセッション テーブル SYN フラッド保護を提供します。ファイアウォールはグローバル テーブルにセッションを保存するため、TCP ハーフオープン セッションの数に制限を設定できます。TCP ハーフオープン セッションは、確立状態に達していないセッションです。VRF 対応ファイアウォールでは、各 VRF の TCP ハーフオープン セッションの数に制限を設定できます。グローバル レベルと VRF レベルの両方で、設定済みの制限に達すると、TCP SYN Cookie はより多くのセッションを作成する前に、ハーフオープンセッションの送信元を確認します。

ファイアウォール TCP SYN Cookie の設定方法

ファイアウォール ホスト保護の設定

ホストのすべてのリソースを引き継ぐために、TCP SYN パケットが単一のホストに送信されます。ホスト保護は、送信元ゾーンに関してのみ設定可能です。宛先ゾーン設定で保護を設定しても、TCP SYN 攻撃から宛先ゾーンが保護されるわけではありません。

ファイアウォール ホスト保護を設定するには、次の作業を実行します。

（注） **show** コマンドは任意の順序で指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **tcp syn-flood rate per-destination** *maximum-rate*
5. **max-destination** *limit*
6. **exit**
7. **zone security** *zone-name*
8. **protection** *parameter-map-name*
9. **exit**
10. **show parameter-map type inspect-zone** *zone-pmap-name*
11. **show zone security**
12. **show policy-firewall stats zone** *zone-name*

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。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Router(config)# parameter-map type inspect-zone zone-pmap`	ゾーン検査タイプ 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 syn-flood rate per-destination** *maximum-rate* 例： `Router(config-profile)# tcp syn-flood rate per-destination 400`	各宛先アドレスの 1 秒あたりの SYN フラッド パケット数を設定します。 • 特定の宛先アドレスに送信される SYN パケットのレートが、宛先ごとの制限を超えた場合、ファイアウォールは宛先アドレスにルーティングされる SYN パケットの SYN Cookie 処理を開始します。
ステップ 5	**max-destination** *limit* 例： `Router(config-profile)# max-destination 10000`	ファイアウォールがゾーンで追跡できる宛先の最大数を設定します。 • *limit* 引数を使って設定された制限を最大宛先が超えた場合、ファイアウォールはSYNパケットをドロップします。
ステップ 6	**exit** 例： `Router(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了して、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 security** *zone-name* 例： `Router(config)# zone security secure-zone`	セキュリティ ゾーンを設定し、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 8	**protection** *parameter-map-name* 例： `Router(config-sec-zone)# protection zone-pmap`	パラメータ マップを使用して指定のゾーンに関する保護を設定します。
ステップ 9	**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を終了し、特権 EXEC モードを開始します。
ステップ 10	**show parameter-map type inspect-zone** *zone-pmap-name* 例：	（任意）ゾーン検査タイプ パラメータ マップの詳細を表示します。

	コマンドまたはアクション	目的
	`Router# show parameter-map type inspect-zone zone-pmap`	
ステップ 11	**show zone security** 例： `Router# show zone security`	（任意）ゾーン セキュリティ情報を表示します。
ステップ 12	**show policy-firewall stats zone** *zone-name* 例： `Router# show policy-firewall stats zone secure-zone`	（任意）パケット制限を超えた、SYN Cookie によって処理された SYN パケットの数を表示します。

ファイアウォール セッション テーブル保護の設定

ファイアウォール上のセッションテーブル リソースを使い果たすことで、そのファイアウォールを通過する正当なトラフィックに対するサービスを拒否することを目的として、TCP SYN パケットがファイアウォール背後の一定範囲のアドレスに送信されます。グローバル ルーティング ドメインまたは VRF ドメインにファイアウォール セッション テーブル保護を設定できます。

グローバル ルーティング ドメインでのファイアウォール セッション テーブル保護の設定

グローバル ルーティング ドメインにファイアウォール セッション テーブル保護を設定するには、次の作業を実行します。

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **tcp syn-flood limit** *number*
5. **end**
6. **show policy-firewall stats vrf global**

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	**parameter-map type inspect global** 例： `Router(config)# parameter-map type inspect global`	グローバル 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 syn-flood limit** *number* 例： `Router(config-profile)# tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 5	**end** 例： `Router(config-profile)# end`	プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 6	**show policy-firewall stats vrf global** 例： `Router# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • また、存在する TCP ハーフ オープン セッションの数もコマンド出力に表示されます。

VRF ドメインでのファイアウォール セッション テーブル保護の設定

VRF ドメインにファイアウォール セッション テーブル保護を設定するには、次の作業を実行します。

（注） **show** コマンドは任意の順序で指定できます。

手順の概要

1. **enable**
2. **configure terminal**

3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **tcp syn-flood limit** *number*
5. **exit**
6. **parameter-map type inspect global**
7. **vrf** *vrf-name* **inspect** *parameter-map-name*
8. **end**
9. **show parameter-map type inspect-vrf**
10. **show policy-firewall stats vrf** *vrf-name*

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	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Router(config)# parameter-map type inspect-vrf vrf-pmap`	VRF 検査タイプ 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 syn-flood limit** *number* 例： `Router(config-profile)# tcp syn-flood limit 200`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 5	**exit** 例： `Router(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了して、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 6	**parameter-map type inspect global** 例： `Router(config)# parameter-map type inspect global`	VRF 検査タイプ パラメータ マップを VRF にバインドし、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 7	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Router(config-profile)# vrf vrf1 inspect vrf-pmap`	パラメータ マップを VRF にバインドします。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Router(config-profile)# end`	プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 9	**show parameter-map type inspect-vrf** 例： `Router# show parameter-map type inspect-vrf`	（任意）VRF 検査タイプ パラメータ マップに関する情報を表示します。
ステップ 10	**show policy-firewall stats vrf** *vrf-name* 例： `Router# show policy-firewall stats vrf vrf-pmap`	（任意）VRF ファイアウォール ポリシーのステータスを表示します。 • また、存在する TCP ハーフ オープン セッションの数もコマンド出力に表示されます。

ファイアウォール TCP SYN Cookie の設定例

ファイアウォール ホスト保護の設定例

次に、ファイアウォール ホスト保護を設定する例を示します。

```
Router(config)# parameter-map type inspect-zone zone-pmap
Router(config-profile)# tcp syn-flood rate per-destination 400
Router(config-profile)# max-destination 10000
Router(config-profile)# exit
Router(config)# zone security secure-zone
Router(config-sec-zone)# protection zone-pmap
```

ファイアウォール セッション テーブル保護の設定例

グローバル パラメータ マップ

次に、グローバル ルーティング ドメインのファイアウォール セッション テーブル保護を設定する例を示します。

```
Router# configure terminal
Router(config)# parameter-map type inspect global
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

検査 VRF タイプ パラメータ マップ

次に、VRF ドメインのファイアウォール セッション テーブル保護を設定する例を示します。

```
Router# configure terminal
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# tcp syn-flood limit 200
Router(config-profile)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# vrf vrf1 inspect vrf-pmap
Router(config-profile)# end
```

ファイアウォール TCP SYN Cookie 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	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『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

ファイアウォール TCP SYN Cookie の設定に関する機能情報

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 :* ファイアウォール *TCP SYN Cookie* の設定に関する機能情報

機能名	リリース	機能情報
ファイアウォール TCP SYN Cookie	Cisco IOS XE リリース 3.3S	ファイアウォール TCP SYN Cookie 機能は、TCP SYN フラッディング攻撃からファイアウォールを保護します。TCP SYN フラッディング攻撃は DoS 攻撃の一種です。通常は、TCP SYN パケットはファイアウォールの背後のターゲット エンド ホストまたはサブネット アドレスの範囲に送信されます。これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。スプーフィング攻撃とは、個人またはプログラムが、データを改ざんして不正な優位性を獲得し、別のものになりすますことです。TCP SYN フラッディングは、ファイアウォールまたはエンド ホスト上のリソースを使い果たすことにより、正当なトラフィックに対する DoS を引き起こすことができます。ファイアウォールおよびファイアウォール背後のエンド ホストでの TCP SYN フラッディングを防ぐには、ファイアウォール TCP SYN Cookie 機能を設定する必要があります。 次のコマンドが導入または変更されました。**parameter-map type inspect-vrf**、**parameter-map type inspect-zone**、**parameter-map type inspect global**、**show policy-firewall stats**、**tcp syn-flood rate per-destination**、**tcp syn-flood limit**。

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。