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、サービス拒否（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 フラッディングでは、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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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。

ファイアウォール TCP SYN Cookie の設定の制約事項

- デフォルト ゾーンは、ゾーン タイプ 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 ゾーンにファイアウォール TCP SYN Cookie 機能を設定できません。
- ファイアウォール TCP SYN Cookie 機能は、加入者単位のファイアウォールをサポートしません。

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 攻撃タイプである 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 フラッド攻撃は、ハッカーが集中的な接続要求でサーバをフラッディングさせると発生します。 このようなメッセージには到達不可の返信アドレスが含まれているため、接続を確立することができません。 結果としての未解決オープン接続の量が最終的にサーバを過負荷にし、有効な要求に対するサービス拒否を招く可能性があるため、正規ユーザが Web サイトへの接続、電子メールへのアクセス、FTP サービスの使用などを実行できなくなります。

SYN フラッド攻撃は次の 2 つのタイプに分かれています。

- ホストのフラッディング：SYN フラッド パケットは、単一ホスト上のすべてのリソースを利用することを目的として、そのホストに送信されます。
- ファイアウォール セッション テーブルのフラッディング：SYN フラッド パケットが、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してリソースが拒否されることを目的として、ファイアウォール背後のアドレス範囲に送られます。

ファイアウォール TCP SYN Cookie 機能により、TCP 接続要求を代行受信して検証して、SYN フラッディング攻撃を防止することができます。 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 は、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）またはゾーンに向かうすべての SYN パケットで機能します。 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 つの半接続をトランスペアレントにバインドします。 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して転送します。

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 ドメインおよび VRF ドメインにセッション 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 テーブルのセッションを保存するため、TCP ハーフ オープン セッション数に対する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 認識ファイアウォールでは、各 VRF の TCP ハーフ オープン セッション数に対する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、設定されている制限に達すると、TCP SYN Cookie は、追加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

ファイアウォールによるホスト保護の設定

TCP SYN パケットが、単一ホスト上のすべてのリソースを占有することを目的として、そのホストに送信されます。ホストの保護は、送信元ゾーンに対してのみ設定できます。宛先ゾーンに対する保護を設定しても、TCP SYN 攻撃から宛先ゾーンは保護されません。

ファイアウォールによるホスト保護を設定するには、次の作業を実行します。

（注） **show** コマンドを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： `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-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 の処理を開始します。
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可能な宛先の最大数を設定します。 • ファイアウォールは、最大宛先が、*limit* 引数を使用して設定された制限を超えた場合に 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。

	コマンドまたはアクション	目的
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対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： `Router# show parameter-map type inspect-zone zone-pmap`	（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。
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、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アドレス範囲に送信されます。 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： `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。

	コマンドまたはアクション	目的
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。 • コマンド出力には、存在する TCP ハーフ オープン セッションの数も表示されます。

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** コマンドを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： `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`	VRF にパラメータ マップをバインドします。

	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。 • コマンド出力には、存在する TCP ハーフ オープン セッションの数も表示されます。

ファイアウォール TCP SYN Cookie の設定例

ファイアウォールによるホスト保護の設定例

次に、ファイアウォールによる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
```

VRF 検査タイプ パラメータ マップ

次に、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 の追加情報

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』

関連項目	マニュアル タイトル
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
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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 の設定の機能情報

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* の設定の機能情報

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 Release 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、TCP 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 フラッディングでは、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することで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。 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**。