分散型サービス妨害攻撃に対する保護

分散型サービス妨害攻撃の防止機能は、グローバル レベル（すべてのファイアウォール セッション）およびVPNルーティングおよび転送（VRF）レベルでのサービス妨害（DoS）攻撃からの保護を提供します。Cisco IOS XE リリース 3.4S 以降のリリースでは、分散型 DoS 攻撃を防ぐために、ファイアウォールセッションのアグレッシブエージング、ファイアウォールセッションのイベント レート モニタリング、ハーフオープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。

分散型サービス妨害攻撃に対する保護に関する情報

ファイアウォール セッションのアグレッシブ エージング

アグレッシブエージング機能により、ファイアウォールは、セッションを積極的にエージングアウトし、新しいセッションのためのスペースを確保することで、ファイアウォールセッションデータベースがいっぱいになるのを防ぐことができます。ファイアウォールはそのリソースを保護するため、アイドル セッションを削除します。アグレッシブ エージング機能により、ファイアウォールセッションが存在できる時間は、タイマーで定義されている時間（エージングアウト時間）よりも短くなります。

アグレッシブ エージング機能には、アグレッシブ エージング期間の開始と終了を定義するしきい値（高位水準点と低位水準点）があります。アグレッシブエージング期間は、セッションテーブルが高位水準点を超えると開始され、低位水準点を下回ると終了します。アグレッシブエージングの期間中、セッションの存続期間は、エージングアウト時間を使用して設定した期間よりも短くなります。ファイアウォールがセッションを終了する時間よりも短い時間で攻撃者がセッションを開始する場合、セッションを作成するために割り当てられているすべてのリソースが使用され、新しいすべての接続が拒否されます。このような攻撃を防ぐには、セッ

ションを積極的にエージングアウトするようにアグレッシブエージング機能を設定できます。この機能はデフォルトで無効に設定されています。

ボックス レベル（ボックスはファイアウォール セッション テーブル全体を示します）および Virtual Routing and Forwarding（VRF）レベルで、ハーフオープン セッションおよび総セッションにアグレッシブ エージングを設定できます。この機能を総セッションに対して設定している場合、ファイアウォールセッション リソースを使用するすべてのセッションが考慮されます。総セッションは、確立されたセッション、ハーフオープンセッション、および不明確セッション データベース内のセッションで構成されます。（確立状態に達していない TCP セッションはハーフオープン セッションと呼ばれます）。

ファイアウォールには 2 つのセッション データベースがあります。1 つはセッション データベースで、もう 1 つは不正確なセッションデータベースです。セッションデータベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が設定されているセッションが含まれます。タプルは、要素の番号付きリストです。不正確なセッション データベースには、5 つ未満のタプル（欠落した IP アドレス、ポート番号など）のセッションが含まれます。ハーフオープン セッションのアグレッシブ エージングでは、ハーフオープン セッションだけが考慮されます。

Internet Control Message Protocol（ICMP）、TCP、および UDP ファイアウォール セッションにはアグレッシブ エージングアウト時間を設定できます。エージングアウト時間は、デフォルトではアイドル時間に設定されます。

イベント レート モニタリング機能

イベント レート モニタリング機能は、ゾーンの事前定義イベントのレートをモニタします。イベント レート モニタリング機能には基本脅威検出機能が含まれています。これはセキュリティデバイスの機能であり、ファイアウォールの内側にあるリソースで発生する可能性のある脅威、異常、および攻撃を検出し、それらに対するアクションを実行します。イベントの基本脅威検出レートを設定できます。特定タイプのイベントの着信レートが、設定されている脅威検出レートを超えると、イベント レート モニタリング機能はこのイベントを脅威と見なし、脅威を阻止するためのアクションを実行します。脅威検出機能は、入力ゾーンでのみイベントを検査します（イベント レート モニタリング機能が入力ゾーンで有効な場合）。

ネットワーク管理者に対し、発生する可能性のある脅威に関する情報がアラート メッセージ（syslog または高速ロガー（HSL））で通知されます。ネットワーク管理者は攻撃ベクトルの検出、攻撃元ゾーンの検出、または特定の動作やトラフィックをブロックするようにネットワーク上のデバイスを設定するなどのアクションを実行できます。

イベント レート モニタリング機能は、次のタイプのイベントをモニタします。

- 基本ファイアウォールチェックが失敗したためにファイアウォールがドロップする：これには、ゾーンまたはゾーンペアのチェック失敗、ドロップアクションを使用して設定されたファイアウォール ポリシーなどがあります。
- レイヤ4インスペクションの失敗が原因でファイアウォールがドロップする：これには、1 番目の TCP パケットが同期（SYN）パケットではないために失敗した TCP インスペクションが含まれることがあります。

- TCP SYN Cookie 攻撃：これには、ドロップされた SYN パケットの数と、スプーフィング攻撃として送信された SYN Cookie の数の集計が含まれることがあります。

イベント レート モニタリング機能は、さまざまなイベントの平均レートとバースト レートをモニタします。各イベント タイプにはレート オブジェクトがあります。レート オブジェクトは、設定可能なパラメータ（平均しきい値、バーストしきい値、期間）が含まれる関連レートにより制御されます。期間はタイム スロットに分割されます。各タイム スロットは期間の 1/30 です。

平均レートは、イベント タイプごとに計算されます。各レート オブジェクトは、30 個の完了済みサンプリング値と、現在進行中のサンプリング期間を保持するための 1 つの値を保持します。計算済みの最も古い値が現在のサンプリング値で置き換えられ、平均が再計算されます。平均レートは各期間で計算されます。平均レートが平均しきい値を超えると、イベント レート モニタリング機能はこれを潜在的な脅威と解釈し、統計情報を更新し、ネットワーク管理者に通知します。

バースト レートは、トークン バケット アルゴリズムを使用して実装されます。各タイムスロットで、トークン バケットがトークンで埋められます。発生する（特定のイベント タイプの）イベントごとに、バケットからトークンが削除されます。空のバケットは、バーストしきい値に到達したことを意味し、管理者が syslog または HSL からアラームを受信します。 **show policy-firewall stats zone** コマンドの出力から、脅威検出統計情報を確認し、ゾーン内でさまざまなイベントに対する潜在的な脅威を理解することができます。

最初に **threat-detection basic-threat** コマンドを使用して、基本脅威検出機能を有効にする必要があります。基本脅威検出機能を設定したら、脅威検出レートを設定できます。脅威検出レートを設定するには、**threat-detection rate** コマンドを使用します。

次の表では、イベント レート モニタリング機能が有効な場合に適用可能な基本脅威検出のデフォルト設定について説明します。

表 *1*: 基本的な脅威の検出のデフォルト設定

パケット ドロップの理由	脅威検出の設定
基本的なファイアウォール ドロップ	平均レート 400 パケット/秒（pps） バースト レート 1600 pps レート間隔 600 秒
インスペクション ベースのファイアウォール ドロップ	平均レート 400 pps バースト レート 1600 pps レート間隔 600 秒
SYN 攻撃ファイアウォール ドロップ	平均レート 100 pps バースト レート 200 pps レート間隔 600 秒

ハーフオープン接続の制限

ファイアウォール セッション テーブルでは、ファイアウォールのハーフオープン接続数を制限できるようになっています。ハーフオープンセッション数を制限することで、ハーフオープン セッションでボックスごとのレベルや Virtual Routing and Forwarding（VRF）レベルでファイアウォール セッション テーブルをいっぱいにしてセッションを確立できないようにする攻撃に対し、ファイアウォールを防御できます。ハーフオープン接続の制限は、レイヤ4プロトコル、Internet Control Message Protocol（ICMP）、TCP、UDP に対して設定できます。UDP ハーフオープンセッション数に対して設定された制限は、TCP や ICMP のハーフオープンセッションには影響しません。設定されたハーフオープンセッションの制限を超えると、すべての新規セッションが拒否され、ログ メッセージが Syslog または高速ロガー（HSL）に生成されます。

次のセッションはハーフオープン セッションと見なされます。

- 3 ウェイ ハンドシェイクを完了していない TCP セッション。
- UDP フローで 1 つのパケットだけが検出された UDP セッション。
- ICMP エコー要求または ICMP タイムスタンプ要求に対する応答を受信していない ICMP セッション。

TCP SYN フラッド攻撃

グローバルの TCP SYN フラッド制限を設定して、SYN フラッド攻撃を制限できます。TCP SYN フラッド攻撃は、サービス妨害（DoS）攻撃の一種です。設定済みの TCP SYN フラッド制限に達すると、ファイアウォールは、さらにセッションを作成する前に、セッションの送信元を確認します。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では、個人やプログラムが偽のデータを使用してネットワーク内のリソースにアクセスしようとします。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乗っ取る可能性があるため、サービス妨害がトラフィックを正当化することになります。TCP SYN フラッド保護は、VRF レベルとゾーン レベルで設定できます。

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 フラッドパケットが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。

分散型サービス妨害攻撃に対する防御の設定方法

ファイアウォールの設定

このタスクの内容は以下のとおりです。

- ファイアウォールを設定します。
- セキュリティ送信元ゾーンを作成します。
- セキュリティ宛先ゾーンを作成します。
- 設定された送信元ゾーンと宛先ゾーンを使用してセキュリティ ゾーン ペアを作成します。
- インターフェイスをゾーン メンバーとして設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** {**icmp** | **tcp** | **udp**}
5. **exit**
6. **parameter-map type inspect global**
7. **redundancy**
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect**
12. **exit**
13. **class class-default**
14. **drop**
15. **exit**
16. **exit**
17. **zone security** *security-zone-name*
18. **exit**
19. **zone security** *security-zone-name*
20. **exit**
21. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
22. **service-policy type inspect** *policy-map-name*
23. **exit**
24. **interface** *type number*
25. **ip address** *ip-address mask*
26. **encapsulation dot1q** *vlan-id*
27. **zone-member security** *security-zone-name*

28. **end**
29. ゾーンを別のインターフェイスにアタッチするには、ステップ21～25を繰り返します。

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	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any ddos-class`	アプリケーション固有の検査タイプ クラス マップを作成し、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4	**match protocol** {**icmp** | **tcp** | **udp**} 例： `Device(config-cmap)# match protocol tcp`	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5	**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を開始します。
ステップ6	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	グローバル検査パラメータ マップを定義し、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7	**redundancy** 例： `Device(config-profile)# redundancy`	ファイアウォールの高可用性を有効にします。
ステップ8	**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、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9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、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 ddos-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** 例： `Device(config-pmap-c)# inspect`	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 モードを開始します。
ステップ 13	**class class-default** 例： `Device(config-pmap)# class class-default`	アクションの実行対象となるデフォルト クラスを設定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 14	**drop** 例： `Device(config-pmap-c)# drop`	同じゾーンの 2 つのインターフェイス間でトラフィックの受け渡しが可能になりす。
ステップ 15	**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 モードを開始します。
ステップ 16	**exit** 例： `Device(config-pmap)# exit`	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、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 17	**zone security** *security-zone-name* 例： `Device(config)# zone security private`	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からなる）ゾーン ペアを作成するには、2つのセキュリティ ゾーンが必要です。
ステップ 18	**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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	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からなる）ゾーン ペアを作成するには、2つのセキュリティ ゾーンが必要です。
ステップ 20	**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 モードを開始します。
ステップ 21	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	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 22	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ddos-fw`	ポリシー マップをトップレベル ポリシーに関連付けます。
ステップ 23	**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 モードを開始します。
ステップ 24	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/0.1`	サブ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 25	**ip address** *ip-address mask* 例： `Device(config-subif)# ip address 10.1.1.1 255.255.255.0`	サブインターフェイスにIPアドレスを設定します。
ステップ 26	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 27	**zone-member security** *security-zone-name* 例： `Device(config-subif)# 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。 • *security-zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの1つを設定する必要があります。

	コマンドまたはアクション	目的
		• インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発のトラフィックを除く）はデフォルトでドロップされます。ゾーン メンバーであるインターフェイスをトラフィックが通過できるようにするには、ポリシー適用対象のゾーン ペアにそのゾーンを含める必要があります。ポリシーの **inspect** または **pass** アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
ステップ 28	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 29	ゾーンを別のインターフェイスにアタッチするには、ステップ 21 ～ 25 を繰り返します。	—

ファイアウォール セッションのアグレッシブ エージングの設定

アグレッシブ エージング機能は、ボックス単位（ボックス単位とは、ファイアウォール セッション テーブル全体を意味します）、デフォルト VRF、および VRF 単位のファイアウォール セッションに設定できます。アグレッシブ エージング機能が動作するには、ファイアウォール セッションのアグレッシブ エージングおよびエージング アウト時間を設定する必要があります。

ファイアウォール セッションのアグレッシブ エージングを設定するには、次の作業を実行します。

ボックス単位のアグレッシブ エージングの設定

ボックス単位とは、ファイアウォールセッションテーブル全体という意味です。**parameter-map type inspect-global** コマンドに続くすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**

4. **per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats 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： `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	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順4と手順5をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

	コマンドまたはアクション	目的
ステップ 4	**per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box max-incomplete 2000 aggressive-aging high 1500 low 1200`	ファイアウォール セッション テーブル内のハーフオープンセッションの上限およびアグレッシブエージング レートを設定します。
ステップ 5	**per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box aggressive-aging high 1700 low 1300`	総セッションのアグレッシブ エージング制限を設定します。
ステップ 6	**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、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	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	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 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになった後、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 9	**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、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバル ファイアウォール統計情報を表示します。

デフォルト VRF のアグレッシブ エージングの設定

max-incomplete aggressive-aging command, it applies to the default VRF. を設定する場合

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します：
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}]
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **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： `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	次のいずれかのコマンドを入力します：
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。

	コマンドまたはアクション	目的
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順5をスキップしてください。 （注） **parameter-map type inspect-global** コマンドを設定する場合は **per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 4	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255`	ハーフオープン ファイアウォール セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 5	**session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総ファイアウォール セッションの合計制限およびアグレッシブ エージング制限を設定します。
ステップ 6	**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、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	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	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 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになった後、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回る

	コマンドまたはアクション	目的
		と、アグレッシブ エージングはディセーブルになります。
ステップ 9	**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、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	グローバル VRF ファイアウォール ポリシー統計を表示します。

ファイアウォール セッションのエージング アウトの設定

ICMP、TCP、またはUDPファイアウォールセッションのエージングアウトを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
5. **exit**
6. **parameter-map type inspect** *parameter-map-name*
7. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect match-any** *class-map-name*
12. **inspect** *parameter-map-name*
13. **end**
14. **show policy-firewall stats vrf** *vrf-pmap-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： `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	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspectglobal`
		グローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順4をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
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、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** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	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。

	コマンドまたはアクション	目的
ステップ 7	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージング アウト時間を設定します。 • また、**tcp finwait-time** コマンドを設定すると、終了（FIN）交換がファイアウォールで検出された後に TCP セッションを管理する時間の長さを指定できます。または **tcp synwait-time** コマンドを設定すると、セッションをドロップする前に TCP セッションが確立状態になるのを待機する時間を指定できます。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングがイネーブルになります。
ステップ 9	**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、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 10	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、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。
ステップ 11	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 12	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	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、特権 EXEC モードを開始します。
ステップ 14	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

 VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 270, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 12
       Half Open Aggressive Aging Period Off, Event Count: 0
```

VRF 単位のアグレッシブ エージングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **parameter-map type inspect-vrf** *vrf-pmap-name*
9. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
10. **session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}]
11. **alert on**
12. **exit**

13. 次のいずれかのコマンドを入力します。
    - **parameter-map type inspect-global**
    - **parameter-map type inspect global**
14. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
15. **exit**
16. **parameter-map type inspect** *parameter-map-name*
17. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
18. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect match-any** *class-map-name*
22. **inspect** *parameter-map-name*
23. **end**
24. **show policy-firewall stats vrf** *vrf-pmap-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： `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	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf ddos-vrf1`	VRF インスタンスを定義し、VRF 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	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:2`	ルートターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	VRF 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 8	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 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 9	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200`	ハーフ オープン セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 10	**session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総セッション制限および総セッションに関するアグレッシブ エージング制限を設定します。 • 総セッション制限は、絶対値またはパーセンテージとして設定できます。
ステップ 11	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 12	**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、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 13	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 14 をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 14	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 15	**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、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 16	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	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 17	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージングアウト時間を設定します。
ステップ 18	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 19	**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、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 20	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、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。
ステップ 21	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションの実行対象となるトラフィック（クラス）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 22	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをディセーブルにします。
ステップ 23	**end** 例： `Device(config-pmap-c)# end`	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、特権 EXEC モードを開始します。
ステップ 24	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 80, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 116
       Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール イベント レート モニタリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **alert on**
5. **threat-detection basic-threat**
6. **threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
7. **threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
8. **threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
9. **exit**
10. **zone security** *security-zone-name*
11. **protection** *parameter-map-name*
12. **exit**
13. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
14. **end**
15. **show policy-firewall stats zone**

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-zone** *zone-pmap-name* 例： `Device(config)# parameter-map type inspect-zone zone-pmap1`	ゾーン検査パラメータ 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	**alert on** 例： `Device(config-profile)# alert on`	ゾーンに関するステートフル パケット インスペクションのアラート メッセージのコンソール表示を有効にします。 • **log** コマンドを使用すると、アラートのロギングを Syslog または高速ロガー（HSL）のいずれかに設定できます。

	コマンドまたはアクション	目的
ステップ 5	**threat-detection basic-threat** 例： `Device(config-profile)# threat-detection basic-threat`	ゾーンの基本脅威検出を設定します。
ステップ 6	**threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール ドロップ イベントの脅威検出レートを設定します。 • **threat-detection rate** コマンドを設定する前に、**threat-detection basic-threat** コマンドを設定する必要があります。
ステップ 7	**threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール インスペクション ベースのドロップ イベントに関する脅威検出レートを設定します。
ステップ 8	**threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate syn-attack average-time-frame 600 average-threshold 100 burst-threshold 100`	TCP SYN 攻撃イベントの脅威検出レートを設定します。
ステップ 9	**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、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 10	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	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 11	**protection** *parameter-map-name* 例： `Device(config-sec-zone)# protection zone-pmap1`	ゾーン検査パラメータ マップをゾーンにアタッチし、ゾーン検査パラメータ マップで設定されている機能をゾーンに適用します。
ステップ 12	**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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 13	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	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 14	**end** 例： `Device(config-sec-zone-pair)# end`	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、特権EXECモードを開始します。
ステップ 15	**show policy-firewall stats zone** 例： `Device# show policy-firewall stats zone`	ゾーン レベルでのポリシー ファイアウォール統計情報を表示します。

ボックス単位のハーフオープン セッション制限の設定

ボックス単位とは、ファイアウォールセッションテーブル全体という意味です。**parameter-map type inspect-global** コマンドに続くすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box max-incomplete** *number*
6. **session total** *number*
7. **end**
8. **show policy-firewall stats 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： `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。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 5 および手順 6 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box max-incomplete** *number* 例： `Device(config-profile)# per-box max-incomplete 12345`	ファイアウォールセッションテーブルのハーフオープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	ファイアウォール セッション テーブルの合計セッション制限を設定します。
ステップ 7	**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、特権 EXEC モードを開始します。
ステップ 8	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバル ファイアウォール統計情報を表示します。

VRF検査パラメータ マップ用のハーフオープンセッション制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-name*
4. **alert on**
5. **max-incomplete** *number*
6. **session total** *number*
7. **exit**
8. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
9. **alert on**
10. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
11. **end**
12. **show policy-firewall stats vrf** *vrf-pmap-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： `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-vrf** *vrf-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査パラメータ 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	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**max-incomplete** *number* 例： `Device(config-profile)# max-incomplete 2000`	VRF ごとのハーフ オープン接続の最大数を設定します。

	コマンドまたはアクション	目的
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	VRF の総セッション制限を設定します。
ステップ 7	**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、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 8	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドのいずれかを使用できます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 10 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は **per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 9	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 10	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	グローバル パラメータ マップに VRF をバインドします。
ステップ 11	**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、特権 EXEC 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 12	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

グローバル TCP SYN フラッド制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box tcp syn-flood limit** *number*
6. **end**
7. **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： `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	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル 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。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定できます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 5 をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box tcp syn-flood limit** *number* 例： `Device(config-profile)# per-box 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 セッションの数を制限します。
ステップ 6	**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、特権 EXEC モードを開始します。
ステップ 7	**show policy-firewall stats vrf global** 例： `Device# 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。 • 存在する TCP ハーフ オープン セッションの数もまたコマンド出力に表示されます。

例

次に、**show policy-firewall stats vrf global** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

分散型サービス妨害攻撃に対する保護の設定例

例：ファイアウォールの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any ddos-class
Router(config-cmap)# match protocol tcp
Router(config-cmap-c)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# redundancy
Router(config-profile)# exit
Router(config)# policy-map type inspect ddos-fw
Router(config-pmap)# class type inspect ddos-class
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# zone security private
Router(config-sec-zone)# exit
Router(config)# zone security public
Router(config-sec-zone)# exit
Router(config)# zone-pair security private2public source private destination public
Router((config-sec-zone-pair)# service-policy type inspect ddos-fw
Router((config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/1/0.1
Router(config-subif)# ip address 10.1.1.1 255.255.255.0
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# zone-member security private
Router(config-subif)# exit
Router(config)# interface gigabitethernet 1/1/0.1
Router(config-subif)# ip address 10.2.2.2 255.255.255.0
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# zone-member security public
Router(config-subif)# end
```

例：ファイアウォール セッションのアグレッシブ エージングの設定

例：ボックス単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# per-box max-incomplete 2000 aggressive-aging 1500 low 1200
Device(config-profile)# per-box aggressive-aging high 1700 low 1300
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：デフォルト VRF のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent
 60
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：ファイアウォール セッションのエージング アウトの設定

```
Device# configure terminal
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-profile)# class type inspect match-any ddos-class
Device(config-profile)# inspect pmap1
Device(config-profile)# end
```

例：VRF 単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# ip vrf ddos-vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# exit
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent
 60
Device(config-profile)# alert on
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-pmap)# class type inspect match-any ddos-class
Device(config-pmap-c)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール イベント レート モニタリングの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect zone zone-pmap1
Device(config-profile)# alert on
Device(config-profile)# threat-detection basic-threat
Device(config-profile)# threat-detection rate fw-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate syn-attack average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# exit
Device(config)# zone security public
Device(config-sec-zone)# protection zone-pmap1
Device(config-sec-zone)# exit
Device(config)# zone-pair security private2public source private destination public
Device(config-sec-zone-pair)# end
```

例：ボックス単位のハーフオープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box max-incomplete 12345
Device(config-profile)# session total 34500
Device(config-profile)# end
```

例：検査 VRF パラメータ マップに対するハーフオープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect vrf vrf1-pmap
Device(config-profile)# alert on
Device(config-profile)# max-incomplete 3500
Device(config-profile)# session total 34500
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# end
```

例：グローバル TCP SYN フラッド制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
```

```
Device(config-profile)# alert on
Device(config-profile)# per-box tcp syn-flood limit 500
Device(config-profile)# end
```

分散型サービス妨害攻撃に対する保護に関する追加情報

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 セキュリティ コマンド リファレンス』
ファイアウォール リソース管理	『*Configuring Firewall Resource Management feature*』
ファイアウォール TCP SYN Cookie	『*Configuring Firewall TCP SYN Cookie feature*』

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

分散型サービス妨害攻撃に対する保護に関する機能情報

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 *2:* 分散型サービス妨害攻撃に対する保護に関する機能情報

機能名	リリース	機能情報
分散型サービス妨害攻撃に対する保護	Cisco IOS XE リリース 3.4S	分散型サービス妨害攻撃に対する保護機能は、ボックス単位レベル（すべてのファイアウォール セッションに対応）と VRF レベルでの DoS 攻撃に対する保護を提供します。DDoS 攻撃を防ぐために、ファイアウォール セッションのアグレッシブ エージング、ファイアウォール セッションのイベント レート モニタリング、ハーフオープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。 次のコマンドが導入または変更されました。**clear policy-firewall stats global**、**max-incomplete**、**max-incomplete aggressive-aging**、**per-box aggressive-aging**、**per-box max-incomplete**、**per-box max-incomplete aggressive-aging**、**per-box tcp syn-flood limit**、**session total**、**show policy-firewall stats global**、**show policy-firewall stats zone**、**threat-detection basic-threat**、**threat-detection rate**、および **udp half-open**。

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。