paloalto
TECHDOCS

DoS およびゾ#ン プロテクションのベストプラクティス

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 6, 2023

Table of Contents

DoS およびゾ#ン プロテクションのベストプラクティス

デプロイメント前、デプロイメント時、デプロイメント後の手順をまとめたこのチェックリストは、サ#ビス拒否 (DoS) とゾ#ン プロテクションのベスト プラクティスの#装に役立ちます。PAN-OS 管理者ガイドへのリンクには、設定の詳細が記載されています。

DoS 攻#は、タ#ゲットサ#バ#にフラッドを生じさせる#一送信元です。分散型サ#ビス拒否 **(DDoS)** 攻#は、タ#ゲットサ#バ#にフラッドを生じさせる複#の送信元です。DDoS 攻#では DoS 攻#よりも多くのセッションの開始が試みられるため、防御により多くのリソ#スが必要です。ファイアウォ#ルはセッションベ#スなので、階層化された DoS/DDoS 防御#略の一部であり、唯一の防御ではありません。

DoS 攻#では、正規ユ#ザ#はデバイスやリソ#スを利用できなります。その原因は、インタ#ネットや設定ミス、あるいはセキュリティ侵害を受けた#部デバイスによるものです。一般的な DoS 攻#では、リソ#ス (メモリ、CPU サイクル、#域幅) を消費するリクエストがタ#ゲットにあふれて、正#なユ#ザ#がそのタ#ゲットを利用できなくなります。WEB サ#バ#やデ#タベ#スサ#バ#など、ユ#ザ#が企業ネットワ#ク外部からアクセスできるインタ#ネットに接#されたデバイスが典型的なタ#ゲットになります。DoS プロテクションのレイヤ# アプロ#チの一環として、Palo Alto Networks のファイアウォ#ルでは 3 つの抑制ツ#ルを提供しています。

ゾ#ン プロテクション プロファイルでは、ゾ#ンに入る新しいセッションの#に#じて個#の入力ゾ#ンが保護されます。このプロファイルでは、ファイアウォ#ルに#する 1 秒あたりの接## (CPS) を制限してフラッド攻#に#する幅#い保護を#現し、偵察 (ポ#ト スキャンとホスト スイ#プ)、パケットベ#スの攻#、およびレイヤ# 2 プロトコルベ#スの攻#から保護します。

DoS プロテクション プロファイルとポリシ# ル#ルは、主要デバイスを新しいセッション フラッドから保護します。分類化ポリシ#では、個#のデバイスを保護します。集約ポリシ#では、デバイスのグル#プを保護します。

分類化 DoS プロテクションの大きな利点は、DoS プロテクション プロファイルの最大レ#トに基づいて、最大 CPS レ#トを超えた送信元 IP アドレスが、ハ#ドウェア ブロック リスト (サポ#トするプラットフォ#ムのソフトウェア リソ#スを節約できる) またはソフトウェア ブロック リストに自動的に追加されることです。ハ#ドウェア ブロック テ#ブルがいっぱいになると、ファイアウォ#ルはソフトウェア ブロック テ#ブルを使用します。

DoS プロテクションでは、個#のサ#バ#がタ#ゲットになるほとんどの攻#が#理され、DoS 防御では不十分な場合は、ゾ#ン プロテクションでゾ#ン全体を#く保護します。DoS プロテクションではブロック テ#ブルを利用するため、ゾ#ン プロテクションよりも消費するリソ#スが少なくて#みます。

パケット バッファ保護—ファイアウォ#ルのパケット バッファを溢れさせようとする#存のセッションからの#一セッション DoS 攻#を防ぎます。パケット バッファ保

護は、プラットフォ#ムがサポ#トしていれば、ハ#ドウェア テ#ブル#の攻#する IP アドレスを隔離します。

> DoS およびゾ#ン プロテクションのベストプラクティスのデプロイメントを計#
> ベストプラクティスによる DoS およびゾ#ン プロテクションのデプロイ
> デプロイ後の DoS およびゾ#ン プロテクションのベストプラクティスに#う

Palo Alto Networks のベスト プラクティス ブック シリ#ズには、復#化、管理者アクセスの保護など、さまざまなテ#マに#するベスト プラクティスのアドバイスが#載されています。

DoS およびゾ#ン プロテクションのベストプラクティスのデプロイメントを計#

このセクションでは、DoS とゾ#ン プロテクションの#装前に理解して、計#すべきベスト プラクティスについて#明します。

- ##準備をしておくべきさまざまな種類の DoS 攻# 。
- 複#の防止メカニズムで、階層を防御する方法。
- ファイアウォ#ルの配置場所。
- 保護するゾ#ンと主要デバイスの 1 秒あたりの通常時とピ#ク時の平均接## (CPS) と、CPU 消費に#するその影響を理解する方法。
- リソ#スを消費するその他のすべての機能が#行されている#態でファイアウォ#ル リソ#スのキャパシティを把握する方法。

プラットフォ#ムでハ#ドウェア ブロック テ#ブルがサポ#トされている場合は、できるだけ分類化 *DoS* プロテクションを使用して、個#の主要サ#バ#の保護を計#してください。分類化 *DoS* 防御は、ハ#ドウェア ブロック テ#ブルを利用して、ブロックされた *IP* アドレスを保存します。そのためり、システム ソフトウェア リソ#スが節約され、パフォ#マンスが向上します。次のプラットフォ#ムは、ハ#ドウェア ブロック テ#ブルをサポ#トしています。

- *PA-3200* シリ#ズ ファイアウォ#ル
- *PA-5200* シリ#ズ ファイアウォ#ル
- *PA-5400* シリ#ズ ファイアウォ#ル
- *PA-7000* シリ#ズ ファイアウォ#ル

プラットフォ#ムのサポ#トに加えて、*DoS* プロテクションにハ#ドウェア ブロック テ#ブルを使用するための#件*:*

- *DoS* プロテクション ポリシ#のアクションは保護とします。
- *DoS* プロテクション プロファイルは、分類化プロファイルとします。
- ドロップ メカニズムとして *RED* を使用するものとします。
- *DoS* プロテクション ポリシ#では、分類化アドレスとして、***source-ip-only*** または ***src-dest-ip-both*** を使用するものとします。

STEP 1 | 各種の DoS 攻#に#する保護を計#してください。

- アプリケ#ション ベ#スの攻#—特定のアプリケ#ションの脆弱性を狙い、正#なユ#ザ#が利用できないよう、リソ#スを消耗させようと試みます。Slowloris攻#がこの例です。
- プロトコル ベ#スの攻# — state-exhaustion 攻#とも呼ばれ、プロトコルの脆弱性を標的にします。SYN フラッド攻#が良くある例です。
- ボリュメトリック攻#—利用できるネットワ#クリソ#ス (特に#域幅) を消耗させて、タ#ゲットをダウンさせ、正#なユ#ザ#による、リソ#スへのアクセスを妨害する大容量の攻#です。UDP フラッド攻#がこの例です。これらの攻#の#生源には、#一の送信元 IP (DoS 攻#) または多#の送信元 IP (DDoS 攻#。送信元 IP アドレスがロ#テ#ションする可能性があり、攻#は高い CPS レ#トと大量のトラフィックの#方、またはいずれかとして#生するおそれがあります) が考えられます。

STEP 2 | レイヤ# アプロ#チを計#して DoS 攻#を防ぎます。

ファイアウォ#ルは DoS 保護#用デバイスには不可能な、アプリケ#ション トラフィックに#する可視性を提供してくれます。DoS 攻#からネットワ#クと主要個#のデバイスを保護するために、必要に#じて、ネットワ#ク境界における大規模な DDoS プロテクションを、個#のデバイスの DoS プロテクションとゾ#ン全体のゾ#ン プロテクションのレイヤ#と組み合わせます。

- #用の大容量 DDoS プロテクションデバイスと境界上のル#タ#、スイッチ、または適切なアクセス制御リスト (ACL) を備えたその他のハ#ドウェアベ#スのパケットドロップ デバイスを、インタ#ネットに接#されたネットワ#ク境界上の最初の保護層として使用します。#用の大容量 DDoS デバイスを境界ファイアウォ#ルの前に配置して、セッションベ#スのファイアウォ#ルでは#理できない大規模な攻#から防御します。
- 個#のゾ#ンをフラッド攻#から保護し、境界で#用の DDoS デバイスを#化するために、ゾ#ン プロテクション プロファイルを#範#に渡る集約的な保護のレイヤ#として適用します。
- パケット バッファ保護を適用し、DoS 攻#によるファイアウォ#ル リソ#スの消費を防ぎます。

- 分類化 DoS プロテクション プロファイルとポリシ#を適用して、#値の高いタ#ゲットを個別に、または小さなグル#プとして保護します (DoS プロテクション プロファイルとポリシ# ル#ル)。
  - CPS を各サ#バ#に制限して、主要インタ#ネット接#サ#バ#を保護します。
  - 疑わしい送信元 (インタ#ネット接#ゾ#ンではなく、#部接#ゾ#ンのみ) からの CPS、あるいは影響を受けた宛先への CPS を制限して、設定ミスの#部ホストや、セキュリティが破られた#部ホストで、DoS 攻#が#行されるのを防ぎます。
  - 特定の送信元 (#部接#ゾ#ンのみ) からの CPS が一定のしきい値に達し、ホストのセキュリティが破られたおそれや、設定が不適切であるおそれが疑われる場合に送信元を監視してアラ#トを#生させます。
  - ファイアウォ#ルがハ#ドウェア ブロック テ#ブルの使用をサポ#トしている場合、ゾ#ン#の特定のデバイスを防御します。
  - ファイアウォ#ルがハ#ドウェア ブロック テ#ブルまたはソフトウェア ブロック テ#ブルの使用をサポ#トしているかどうかに#係なく、ログ#の攻#に#連付けられた IP アドレスを可視化します。
- 集約 DoS プロテクション プロファイルとポリシ#では、必要に#じて、主要サ#バ#のグル#プに#範#な追加保護レイヤ#が提供されます。ほとんどの場合、個#の主要サ#バ#には分類化 DoS プロテクション、ゾ#ン全体にはゾ#ン プロテクションで十分であり、設定の複#さを回避できます。さらに、集約 DoS プロテクション ログには、攻#に#連付けられた IP アドレスは表示されず、ポリシ#ではハ#ドウェア ブロック テ#ブルを利用されません。攻#している IP アドレスを可視化するには、分類化 DoS プロテクションを使用します。

  集約 *DoS* プロテクションはゾ#ン プロテクションとは異なり、ゾ#ン プロテクションではゾ#ン全体が攻#から防御されますが、集約 *DoS* プロテクションではゾ#ン#の主要デバイスの小さなグル#プが保護されます。集約 *DoS* プロテクションは、分類化 *DoS* プロテクションとは異なり、分類化 *DoS* プロテクションでは個#のデバイスごとに *CPS* しきい値が設定されますが、集約 *DoS* プロテクションではデバイスのグル#プに *CPS* しきい値が設定されます。

さまざまなシナリオでどちらを使用すればよいか判#できるよう、分類化 DoS プロテクションと集約 DoS プロテクションの違いをよく調べてください。

ゾ#ン プロテクションと **DoS** プロテクションを#用するためのしきい値計# — プラットフォ#ムでハ#ドウェア ブロック テ#ブルがサポ#トされている場合は、DoS プロテクションが最初にアクティベ#トされ、必要に#じてゾ#ン プロテクションによって追加の防御層が機能するように、分類化 DoS プロテクションしきい値をゾ#ン プロテクションしきい値よりも低く設定する計#をたててください。主要デバイスのグル#プ (Web サ#バ#やインタ#ネットに接#されたファイル サ#バ#など) の保護を最優先する場合は、分類化 DoS プロテクションのしきい値よりも高く、ゾ#ン プロテクションのしきい値よりも低く設定したしきい値で集約 DoS プロテクションを追加してください。(これにより、必要に#じて、分類化 DoS プロテクション

が最初にアクティベ#トされ、集約 DoS プロテクションが 2 番目にアクティベ#トされて、ゾ#ン プロテクションが 3 番目にアクティベ#トされます。)

プラットフォ#ムでハ#ドウェア ブロック テ#ブルをサポ#トされていない場合でも、同じ方法を適用しますが、ハ#ドウェア ブロック テ#ブルに#する負担#減の利点はありません。

STEP 3 | できるだけ保護するリソ#スの近くにファイアウォ#ルを配置します。

ファイアウォ#ルはセッションベ#スなので、#百万の CPS まで#張することはできません。保護するリソ#スにファイアウォ#ルを近づけるほど、トラフィックで消費されるセッション#とファイアウォ#ル リソ#ス#を少なくできます。

- ACL を使用して DoS トラフィックをドロップする#用の大容量境界 DDoS デバイス、境界ル#タ#、またはスイッチの背後に、境界ファイアウォ#ルを配置します。これにより、エンタ#プライズ ネットワ#クをゾ#ンに分割し、それらのゾ#ン#のデバイスを保護するファイアウォ#ルが保護されます。大量のトラフィックに##するためには、ファイアウォ#ルが境界に近いほど、高いキャパシティが求められます。
- ネットワ#ク ゾ#ンの分割を#討します。セグメント分けが大#把過ぎる場合は、各ゾ#ンを小さくすることを#討してください。ゾ#ンが小さくなると、マルウェアの#方向の移動の防御機能が向上し、トラフィックに#する可視性が#し、#部 DoS 攻#の最大範#を削減できるなど、多くの面でセキュリティ向上につながります。

STEP 4 | フラッドのしきい値によって意#せずトラフィックが押さえ#まれたり、DoS 攻#が見過ごされないよう、保護する個別の主要デバイスやゾ#ンの平均時とピ#ク時の CPS のベ#スラインを測定して、ファイアウォ#ルのキャパシティを#討してください。復#化、URL フィルタリング、GlobalProtect など、通常のリソ#ス消費機能で、トラフィックのピ#ク時と通常のピ#ク時に#行される トラフィック回#を測定します。

- ゾ#ン プロテクション プロファイルのしきい値については、PAN-OS 10.0 以降を#行している場合は、AIOps クラウド サ#ビスのゾ#ン プロテクション プロファイルしきい値推#アラ#トを使用します。ここでは、システム テレメトリにより、平均時と平均ピ#ク CPS 値の正確な推定値が得られます。サ#ビスのファイアウォ#ルと Panorama にサインアップします。(PAN-OS 10.2.1 以降では、Panorama 用の AIOps プラグインをインスト#ルして、設定を管理#象のファイアウォ#ルにプッシュする前に、事前にセキュリティ チェックを#施できます。)

  AIOps を使用できない場合は、少なくとも 1 週間の#業時間#にファイアウォ#ル ゾ#ンごとに、ファイアウォ#ル ACC とその他のツ#ルで、ベ#スライン CPS 測定値を測定してください。デ#タ#集期間が長いほど精確な測定値が得られます。個#のゾ#ンごとに通常時とピ#ク時の CPS を測定して、ゾ#ンごとに適切なゾ#ン プロテクション フラッドしきい値を設定します。

- DoS プロテクションの場合、主要デバイス (タ#ゲット候補) の平均時とピ#ク時の CPS のベ#スラインを測定します。同じツ#ルを使用して、バッファの使用率を調べます。
  - #業時間中、少なくとも 1 #業週間にかけてインタ#ネットに接#された重要なデバイスの CPS のベ#スラインを測定します。デ#タ#集期間が長いほど精確な測定値が得られます。
  - アプリケ#ション チ#ムと協力し、通常およびピ#ク時のサ#バ#への CPS、そのサ#バ#がサポ#トできる最大 CPS を把握します。
  - 重要なデバイスの宛先 IP アドレスに基づいてファイアウォ#ルのトラフィックおよび脅威ログをフィルタリングし、通常およびピ#ク時のセッション アクティビティのベ#スラインを測定します。
  - トラフィックが#えたり、トラフィック パタ#ンが#わったり、普段ネットワ#ク上で使用しないアプリケ#ションを使ったりする特別なイベント、四半期#のイベント、年次のイベントを考慮してください。

  ゾ#ンと個#のデバイスの通常のピ#ク CPS の把握は、ゾ#ン プロテクション プロファイルと DoS プロテクション プロファイルで適切なしきい値を設定するために重要です。過度に積極的な値を設定すると (しきい値の設定値が低すぎるか、CPS の設定#が少なすぎる)、アクティビティのピ#ク時に正#なトラフィックが想定外で抑制されてしまうおそれがあります。過度に受け身な値を設定すると (しきい値の設定値が高すぎるか、CPS の設定#が多すぎる)、DoS 攻#の#減に十分な保護が得られず、保護しようとしているリソ#スに影響が出るおそれがあります。
- ファイアウォ#ルのキャパシティおよび他の機能が消費するリソ#ス（CPU とメモリ）を確認し、DoS 保護で使用できる分を把握してください。トラフィックのピ#ク時と通常時に#行される他の通常のリソ#ス消費機能で CPS を測定します。
  - Panorama でファイアウォ#ルを管理する場合は、デバイス監視で CPS 値を測定します。また、各ファイアウォ#ルで典型的に利用できるキャパシティを把握する際に役立つ、90 日間の平均およびピ#ク時の CPU 使用#況の傾向をデバイス監視で確認することもできます。

    Panorama のデバイス監視を使用できず、SNMPを使用する場合は、お使いの管理ツ#ルを使って次の 3 つの MIB をポ#リングし、CPS の履#デ#タを#集できます。PanZoneActiveTcpCps、PanZoneActiveUdpCps、および PanZoneOtherIpCps。

    > *MIB では C2S セッション セグメントと S2C セッション セグメントが 1 つのセッションとしてではなく別#にカウントされるため、MIB では#際の CPS 値の 2 倍の値が表示されます。たとえば、MIBのCPS値が10,000の場合、#際のCPS値は5,000になります。*
  - Wireshark、NetFlow などのサ#ドパ#ティ制のツ#ルを使用し、ネットワ#ク トラフィックを#集#分析します。
  - CPS 情報の#集、##的な監視、ログ情報のマイニングを自動化するスクリプトを使用することを#討してください。

STEP 5 | スイッチ、ル#タ#、または#用の DDoS デバイスなどのアップストリ#ム デバイスによって、ファイアウォ#ルが攻#されているときに追加のフィルタリングとブロックが自動的に#行されて、ファイアウォ#ル リソ#スが保護されるよう、ログ#送トリガ#(トラフィック一致基準) を設定します。

ログ#送トリガ#を設定し、トリガ##件が#生すると、アップストリ#ム デバイスで攻#に#するアクションが#行されるようファイアウォ#ルから API 呼び出しが自動的に送信されます。

アップストリ#ム デバイスまたはデバイスと API 呼び出し (アップストリ#ム デバイスまたはデバイスが#行するアクション) を HTTP サ#バ# プロファイル (デバイス > サ#バ#プロファイル > **HTTP**) で指定します。サ#バ#タブでアップストリ#ム デバイスを指定し、ペイロ#ド形式タブのペイロ#ドフィ#ルドで API 呼び出しを指定します。

ログ#送プロファイル (オブジェクト > ログ#送) 一致リスト フィルタ#に API 呼び出しをトリガ#するトラフィック一致#件を指定します。

- 特定の種類の攻#でトリガ#するには、フィルタ##理またはブロックするトラフィックの脅威ログに一致するフィルタ#をフィルタ# ビルダ#で作成します。たとえば、次のフィルタでは、FTP ブル#ト フォ#ス ログイン、HTTP リクエスト ブル#ト フォ#ス攻#、および Apache Benchmark ブル#ト フォ#ス DOS 攻#の脅威の各 ID に##する 3 つの脅威 ID を指定します。
  - **(**脅威 **eq 40001)** または **(**脅威 **eq 39290)** または **(**脅威 **eq 35075)**

  これらの脅威シグネチャでトリガ#するようにログ#送を設定すると、ファイアウォ#ルでは、問題のあるトラフィックのフィルタリングまたはブロックを要求する API 呼び出しを、指定されたアップストリ#ム デバイスに送信できます。
- 特にブロック テ#ブルが小さいプラットフォ#ムでファイアウォ#ル リソ#スを攻#から保護するには、DoS 攻##件下でトリガ#するフィルタ#をログ#送プロファイルのフィルタ# ビルダ#で作成して、アップストリ#ム デバイスで問題のトラフィックにファイアウォ#ル ブロック リスト リソ#スを消費させず、ブロックさせます。

  アップストリ#ム デバイスの容量をチェックして、トラフィック負荷を#理できることを確認します。

  DoS トラフィック#件でトリガ#するようにログ#送を設定すると、ファイアウォ#ルでは、そのトラフィックを null ル#トに送信してサイレントに破棄するよう、指定されたアップストリ#ム デバイスに要求する API 呼び出しを送信できるため、ファイアウォ#ル ブロック テ#ブル リソ#スの節約になります。

ベストプラクティスによる DoS およびゾ#ン プロテクションのデプロイ

DoS およびゾ#ン プロテクションでは、個別の主要サ#バ# (DoS プロテクション) とゾ#ン (ゾ#ン プロテクション) がアプリケ#ション ベ#スのフラッド攻#とプロトコル ベ#スのフラッド攻#から保護されます。また、インタ#ネット境界にある#用のDDoS防止デバイスに#く、ボリュメトリック攻#に#する次の防御層にもなります。

デプロイメントの開始前に、主要サ#バ#とゾ#ンの平均接##とピ#ク時接## (CPS) を測定して、ベ#スラインの通常 *CPS* とピ#ク *CPS* を把握して、インテリジェントなフラッドしきい値を設定します。

デプロイメントには次のものが含まれます。

- ゾ#ン プロテクション ファイルの作成
- DoSプロテクション ポリシ#のル#ルとプロファイルの適用
- グロ#バルパケットバッファ保護の有#化
- イングレスゾ#ンごとのパケットバッファ保護の有#化
- ベストプラクティスの脆弱性防御プロファイルをセキュリティ ポリシ#の許可ル#ルに添付

STEP 1 | ゾ#ン プロテクション プロファイル（ネットワ#ク > ネットワ#クプロファイル > ゾ#ンプロテクション）を作成し、各ゾ#ンを防御するために適用します。

ゾ#ン プロテクション プロファイルは入力ゾ#ン#の新規セッションに適用され、フラッド攻#、偵察行#（ポ#トスキャンおよびホスト スイ#プ）、パケット ベ#スの攻#、レイヤ# 2 のプロトコル ベ#スの攻#を防ぎます。

- TCP SYN、UDP、ICMP、ICMPv6、およびその他の IP 新規セッション フラッドによってファイアウォ#ルが影響を受けないようにトラフィックを抑制して、アラ#ム レ#ト、アクティベ#ト、最大の各しきい値を設定します。 SYN フラッドのアクションを設定します。

  CPU 使用量を測定して、ファイアウォ#ルで。*DoS*、ゾ#ン プロテクション、そして、復#化など、*CPU* サイクルを消費するその他の機能を確#にサポ#トします。

  Panorama を使用している場合、ヘルス モニタ# ***(Panorama*** > 管理#象デバイス > ヘルス*)* で、指定期間の *CPU* とメモリの消費量を確認します。*Panorama* がない場合は、#行中のリソ#ス モニタ#を表示を#行し、*CPU* 使用量量を測定するタイムフレ#ムを指定します。*SNMP* を使用する場合は、監視システムから情報を取得できます。

  TCP SYN フラッドの場合は、アクションをランダム早期ドロップまたは **SYN Cookie** に設定して、フラッドしきい値を超えたときにファイアウォ#ルがセッションを ドロップする方法を制御します。メソッド間にはトレ#ドオフがあります。

  - **SYN Cookie**—不正 SYN-ACK ハンドシェイクでは、SYN Cookie によってトラフィックがドロップします。SYN Cookie では正#なトラフィックはドロップされず、ハンドシェイク プロトコルに違反するトラフィックのみがドロップされます。したがって、ドロップされるのは不正なトラフィックのみなので、RED よりも本質的に公平な#きをします。SYN Cookie は、フラッドしきい値の設定が簡#なため、デプロイも簡#です。ただし、SYN Cookie では、より多くのリソ#スが消費されるます。したがって、SYN Cookie を使用するときは、ファイアウォ#ルの CPU とメモリの使用率を監視してください。
  - ランダム早期ドロップ (RED)—設定したアクティベ#トしきい値と最大 CPS しきい値を基準にした確率曲線上で、トラフィックを無差別にドロップします (脅威に基づいていないため、#意のあるトラフィックと正#なトラフィックの#方がドロップされます)。CPS がアクティベ#トしきい値 に達すると、ファイアウォ#ルでセッションのドロップが開始します。セッション#が#えると、最大セッションしきい値に達するまでドロップ レ#トが#加します。最大 CPS レ#トを超えるすべての新しいセッションは、CPS レ#トが最大しきい値未#になるまでドロップされます。アクティベ#トしきい値と最大 CPS しきい値の差が大きいほど、セッションがアクティベ#トしきい値から最大しきい値への#加するにつれて、ドロップ確率の上昇率は低下します。

  SYN Cookie と RED のどちらを選#するかは、使用できるファイアウォ#ル リソ#ス、ゾ#ンでサポ#トするセッションの#、およびトラフィックをどの程度積極的にドロップする

かの問題です。正#なトラフィックに#して、SYN Cookie では影響が#えられず、RED では影響が#えられるため、まずは SYN Cookie から始めて CPU とメモリの使用#況を監視し、SYN Cookie がシステムリソ#スを消費しすぎる場合は RED に切り替えることをお#めします。

SYN Cookie または *RED* のゾ#ン プロテクションしきい値を設定するときは、正#なセッションの通常時およびピ#ク時の負荷を受け入れるだけのに十分に高い値で、かつ、フラッドを防ぐのに十分に低い値に設定します。ゾ#ン全体の保護が目的なので、ゾ#ン プロテクションのしきい値は、分類した *DoS* プロテクションのしきい値よりも高く、集約 *DoS* プロテクションのしきい値よりわずかに高く設定します。この方法では、最初に個#の主要タ#ゲットを#象に分類した *DoS* プロテクションがアクティベ#トされ、主要タ#ゲットのグル#プを#象に *2* 番目に集約 *DoS* プロテクション *(*使用する場合*)*、*3* 番目にゾ#ン プロテクションがアクティベ#トされます。

SYN Cookie は、不正な SYN ハンドシェイクのトラフィックをドロップします。アクティベ#トしきい値と最大 しきい値では、不正な SYN ハンドシェイクのドロップを開始するタイミング (アクティベ#ト) と SYN トラフィックの受け入れを停止するタイミング (最大) を決定します。SYN Cookie のしきい値:

- アラ#ム レ#ト—通常の#動に##できるように、ゾ#ンの平均 CPS レ#トよりも 15 ~ 20% 高く設定します。
- アクティベ#ト—SYN Cookie では不正なトラフィックのみが防御され、正#なトラフィックは防御されません。したがって、不正な SYN ハンドシェイクがあるトラフィックの許可を防ぐため、SYN Cookie はただちにアクティベ#トします (デフォルト値 0 CPS のしきい値)。
- 最大—SYN Cookie は不正なトラフィックのみが防御されます。したがって、リソ#スを大量に消費する他のアクティブな機能を考慮して、低いしきい値で良好な SYN トラフィックが不必要にブロックされないよう、ファイアウォ#ル プラットフォ#ムの最大 CPS キャパシティに最大値を設定します。(SYN Cookie ではアクティベ#トしきい値で不正なトラフィックがドロップされるため、最大値を下げても不良トラフィックが積極的にドロップされるわけではありません)。

  SYN Cookie が最大しきい値に達すると、ファイアウォ#ルでは *SYN* フラッドの方向のすべてのセッションが *5* 分間ブロックされます。反#方向のトラフィックは、影響を受けません。*SYN Cookie* のブロック時間は設定できません。

RED しきい値:

- アラ#ム レ#ト—通常の#動に##できるように、ゾ#ンの平均 CPS レ#トよりも 15 ~ 20% 高く値を設定します。
- アクティベ#ト—フラッド#減のために接#のドロップを開始するアクティベ#トは、ゾ#ンの通常のピ#ク CPS レ#トのすぐ上に設定します (通常のピ#ク アクティビティ#のトラフィックのドロップは開始しません)。この値は、通常はアラ#ム レ#トより 15#20% 高くなります。

- 最大—ファイアウォ#ルの CPU 使用率に基づいて [最大レ#ト] を設定します。ファイアウォ#ルの CPU 使用率が 50% を超える場合は、[最大 CPS] をアクティベ#トレ#トの 2 倍に設定してください。ファイアウォ#ルの CPU 使用率が 50% 未#の場合は、[最大 CPS] をアクティベ#トレ#トの 3 倍に設定し、CPU 使用率を監視してください。CPU 使用率が高すぎる場合は、[最大値] をアクティベ#トレ#トの 2 倍に下げてください。この最大値しきい値を超えると、CPS レ#トがこの値を下回るまで新しい接#がブロックされます。

  複#のデ#タプレ#ン プロセッサ（*DP*）を持つファイアウォ#ルは、*DP* 全体に接#を分配します。通常、ファイアウォ#ルは *CPS* のしきい値設定を *DP* 全体に#して均等に割ります。例えば、ファイアウォ#ルに *5* つの *DP* があり、***Alarm Rate***（アラ#ム レ#ト）を *20,000 CPS* に設定する場合、各 *DP* の***Alarm Rate***（アラ#ムレ#ト）が *4,000 CPS*（*20,000 / 5 = 4,000*）になるため、*DP* の新規 *CPS* が *4,000* を超えると、その *DP* の*Alarm Rate*（アラ#ム レ#ト）のしきい値が#動します。

  ログ > 脅威を監視し、ログタイプのフラッドをフィルタリングしてアラ#ムを表示します。

- 必要に#じてしきい値を監視して調整します。

- すべてのゾ#ンで偵察行#防御を 有#にして、ホスト スイ#プ、さまざまな種類のスキャン、およびその他の偵察活動をブロックします。偵察行#をブロックする前に分析目的でいくつかのパケットをログに記#するためのデフォルト イベントの**Threshold**（しきい値）を保持します。**Source Address Exclusion**（送信元アドレスの除外）を使用し、ネットワ#クの脆弱性をテストする#部グル#プ許可します。

- #意のあるパケットをドロップしてパケット ベ#スの攻#を防止します。

  - **IP Drop (IP** ドロップ**)—Unknown (**未知**)**および**Malformed (**不正な形式**)**のパケットをドロップします。ソ#ス ル#ティングにより、宛先 IP アドレスを一致#件として使用するセキュリティ ポリシ#ル#ルを攻#者がバイパスできるようになるため、**Strict Source Routing**（#格なソ#ス ル#ティング）および**Loose Source Routing**（ル#ズ ソ#ス ル#ティング）パケットをドロップします。#部ゾ#ンの場合、**Spoofed IP address**（なりすまし **IP** アドレス）のパケットをドロップし、入力部分で送信元アドレスを確#にファイアウォ#ルのル#ティングテ#ブルにマッチさせます。

  - **TCP** ドロップ—デフォルトのドロップ選#肢の **TCP SYN with Data** と **TCP SYNACK with Data** はそのままで、不一致な重複 **TCP** セグメントとハンドシェイクをスプリットを選#して、ストリップ オプションの **TCP** タイムスタンプを有#にします。

    ゾ#ン上でトンネル コンテンツ#査を設定し、***Rematch Sessions***（セッションの再マッチ）を有#化する場合、そのゾ#ンに#してのみ***Reject Non-SYN TCP***（非 ***SYN TCP*** を拒否）を無#化し、トンネル コンテンツ#査ポリシ#を有#化したり編集したりしても、ファイアウォ#ルが#存のトンネル セッションをドロップしないようにします。

- **ICMP Drop**（**ICMP** ドロップ）—ICMP を使用するかどうか、またどのように使用するのかによって、ブロックする#象が異なります。
- **IPv6 Drop**（**IPv6** ドロップ）—コンプライアンスが#わる場合、コンプライアンスを#たしていないル#ティング ヘッダ#、#張子などを持つパケットをドロップします。
- **ICMPv6 Drop**（**ICMPv6** ドロップ）—コンプライアンスが#わる場合、必ずセキュリティ ポリシ# ル#ルにマッチしない特定のパケットをドロップします。

- ネットワ#ク上で使用しないプロトコルを拒否し、レイヤ# 2 および vwire インタ#フェイス上のレイヤ# 2 のプロトコル ベ#スの攻#を防止するプロトコル保護を有#化します。
  - ファイアウォ#ルの前面にあるレイヤ#3デバイス#由でパブリックインタ#ネットに面しているvwireインタ#フェイスの場合、インタ#ネットに面しているゾ#ンで**Protocol Protection**（プロトコル保護）を有#にします。
  - レイヤ#2ゾ#ンの場合は、インタ#ネットに面しているゾ#ンの**Protocol Protection**（プロトコル保護）を有#化します。#部レイヤ#2ゾ#ンでは、**Protocol Protection**（プロトコル保護）を有#にして、**Include List**（包含リスト）を使って、使用するレイヤ#2プロトコルのみを許可し、その他のプロトコルは自動的に拒否します。（リストにないすべてのプロトコルを許可する、**Exclude List**（除外リスト）は使用しないでください。）**Protocol Protection**（プロトコル保護）を設定しない場合、すべてのレイヤ# 2 プロトコルが許可されます。
- ゾ#ン プロテクション プロファイルフィ#ルドの各ゾ#ン（ネットワ#ク > ゾ#ン）にプロファイルを付#します。

STEP 2 | 特に WEB サ#バ#やデ#タベ#スサ#バ#など、ユ#ザ#がインタ#ネットからアクセスする、攻##象になりやすい重要な特定のシステムに#してDoS 保護を適用します。

DoS プロテクションは、ゾ#ン#の主要タ#ゲットを個別に保護する防御レイヤ#を提供します。ゾ#ン プロテクション CPS しきい値を設定してゾ#ン全体を保護すると、ほとんどのデバイスで個#に#理できる量よりもはるかに高い集約 CPS レ#トを受け取ることができます。主要サ#バ#を個別にタ#ゲットにした攻#には、ゾ#ン プロテクションをアクティベ#トするだけの十分な高い CPS レ#トがない可能性があります。そのため、ゾ#ン#の主要タ#ゲットには、DoS プロテクションを設定します。DoS プロテクションは、次の要素で設定します。

- DoS 攻#から保護するトラフィックを定義するデバイス、ユ#ザ#、ゾ#ン、サ#ビスを指定する DoS プロテクション ポリシ# ル#ル。
- DoS プロテクション プロファイルには、さまざまなタイプのトラフィックにフラッドしきい値を設定します。

DoS プロテクション プロファイルは、DoS プロテクション ポリシ# ル#ルに追加します。このプロファイルは、ポリシ# ル#ルで定義されたトラフィックにファイアウォ#ルを適用する CPS しきい値を定義します。

分類化/集約 DoS プロテクション プロファイルを設定し、そのいずれか、または#方を DoS プロテクション ポリシ# ル#ルに適用します (各ポリシ# ル#ルにはいずれか 1つのプロファイル タイプを設定できます)。分類化プロファイルでは、ル#ルで指定したデバイスごとに適

用されるしきい値を設定します。プラットフォ#ムのハ#ドウェア ブロック テ#ブルを使用します。集約プロファイルでは 、ル#ルで指定したデバイスの結合グル#プに適用されるしきい値を設定します (グル#プの合計 CPS レ#トがしきい値を超えると DoS プロテクションがアクティベ#ト)。ソフトウェア テ#ブルを使用します。

ゾ#ン プロテクションと同#に、アクションでは、SYN Cookie またはランダム早期ドロップ (RED) に設定して、ファイアウォ#ルによる攻#の#減方法を調整できます。 どちらを選#するかは、使用できるファイアウォ#ルリソ#ス、ゾ#ンでサポ#トするセッションの#、そしてトラフィックをどの程度積極的にドロップするかで決めます。システムリソ#スの使用#況を監視し、SYN Cookie で過度のリソ#スが消費される場合は、RED に切り替えてください。ファイアウォ#ルの前面に#用の DDoS 保護デバイスがない場合、必ず RED を使用してください。

DoS プロテクションしきい値を設定するときは、主要タ#ゲットの個別の保護が最初にアクティベ#トされるように、分類化 *DoS* プロテクションしきい値を最低値に設定してください。集約 *DoS* プロテクションを使用する場合は、分類化 *DoS* プロテクションのアクティベ#トには不十分でも、ゾ#ン プロテクションをアクティベ#トするほどではない場合にのみ、集約 *DoS* プロテクションがアクティベ#トされるように、それらのしきい値を分類化 *DoS* プロテクションしきい値よりも高く、そしてゾ#ン プロテクションしきい値よりも低く設定してください。

- 保護する主要デバイスまたは主要デバイスのセットごとに、DoSプロテクション プロファイル (オブジェクト > セキュリティ プロファイル > **DoS** プロテクション) を作成します。SYN、UDP、ICMP、ICMPv6、その他の IP フラッドのしきい値および SYN フラッドの**Action**（アクション）を設定します。ネットワ#クはどれも異なるため、デフォルトのしきい値が適切でないことも良くあります。保護中のデバイスのキャパシティに合わせてしきい値を決定してください。

  ファイアウォ#ルの CPU 使用量を測定し、*DoS*、ゾ#ン プロテクション、復#化などの *CPU* サイクルを消費するその他の機能を、ファイアウォ#ルでサポ#トできることを確認します。

  SYN フラッドのアクションとして SYN Cookie は、次のように設定します。

  - **Alarm Rate**（アラ#ム レ#ト）—分類化プロファイルの場合、通常の#動を考慮して CPS レ#トをデバイスの平均 CPS レ#トよりも 15 ~ 20% 高く設定します。

    集約プロファイルの場合、グル#プの平均 CPS レ#トよりも 15 ~ 20% 高く設定します。
  - アクティベ#ト レ#ト—分類化プロファイルでは、それぞれデバイスに特定の CPS 制限が適用されます。CPS を徐#に調整しなくても、アクティベ#ト レ#トを最大レ#トと同じしきい値に設定できるよう、制限は個#のデバイスのキャパシティに基づいて設定してください。**Max Rate**（最大レ#ト）に達する前にトラフィックをドロップし始めたい

場合のみ、**Activate Rate**（アクティベ#ト レ#ト）を**Max Rate**（最大レ#ト）よりも低く設定します。

集約プロファイルの場合は、通常のアクティビティで想定されるトラフィックがドロップされるのを防ぐため、グル#プの通常のピ#ク CPS レ#トの値からすぐ上にしきい値を設定してください。その場合、しきい値は、一般に、アラ#ムレ#トを 15#20% 上回る値になります。

- 最大レ#ト—分類化プロファイルの場合、最大トラフィック負荷を受け入れてもフラッドしないように、最大レ#トを保護#象のデバイスの最大キャパシティに設定してください。

  集約プロファイルの場合、このしきい値は、グル#プ キャパシティの 80 ~ 90% に設定してください。CPS がしきい値に達すると、ファイアウォ#ルは**Block Duration**（ブロック期間）の間、新規接#をドロップします。

- ブロック期間—同じ送信元の正#なセッションに長くペナルティを課すことなく、攻#中のセッションをブロックするには、デフォルト値 (300 秒) を設定してください。

- 必要に#じてしきい値を監視して調整します。

アクションとしての RED は、次のように設定します。

- **Alarm Rate**（アラ#ム レ#ト）—分類化プロファイルの場合、通常の#動を考慮して CPS レ#トをデバイスの平均 CPS レ#トよりも 15 ~ 20% 高く設定します。

  集約プロファイルの場合、グル#プの平均 CPS レ#トよりも 15 ~ 20% 高く設定します。

- アクティベ#ト レ#ト—分類化プロファイルの場合、タ#ゲットの通常のピ#ク CPS レ#トのすぐ上の値にしきい値を設定して、接#のドロップと攻#の#減を開始します (通常のピ#クアクティビティ#にあるトラフィックがドロップされるほどしきい値を低く設定しないでください)。通常はアラ#ムレ#トを 15#20% 上回る値にします。

  集約プロファイルの場合は、通常のアクティビティで想定されるトラフィックがドロップされるのを防ぐため、グル#プの通常のピ#ク CPS レ#トの値からすぐ上にしきい値を設定してください。その場合、しきい値は、一般に、アラ#ムレ#トを 15#20% 上回る値になります。

- 最大レ#ト—分類化プロファイルおよび集約プロファイルでは、ファイアウォ#ルの CPU 使用率に基づいて最大レ#トを設定します。ファイアウォ#ルの CPU 使用率が 50% を超える場合は、[最大 CPS] をアクティベ#トレ#トの 2 倍に設定してください。ファイアウォ#ルの CPU 使用率が 50% 未#の場合は、[最大 CPS] をアクティベ#トレ#トの 3 倍に設定し、CPU 使用率を監視してください。CPU 使用率が高すぎる場合は、[最大値]

をアクティベ#トレ#トの 2 倍に下げてください。このしきい値を超えると、CPS レ#トがしきい値を下回るまで新しい接#はブロックされます。

最大レ#トを個#のデバイスのキャパシティ (分類化) またはグル#プのキャパシティの*80#90%* (集約) に設定して、タ#ゲットの#理可能#より多くの接#は許可しないようにします。

CPS がしきい値に達すると、ファイアウォ#ルはブロック期間の間、新規接#はドロップされます。

- ブロック期間—同じ送信元の正#なセッションに長くペナルティを課すことなく、攻#中のセッションをブロックするには、デフォルト値 (300 秒) を設定してください。
- 必要に#じてしきい値を監視して調整します。

- DoSプロテクション ポリシ# ル#ル (ポリシ# > **DoS**プロテクション) を作成します。各ル#ルをできるだけ具体的なものにし、ファイアウォ#ルの CPU とメモリ リソ#スを節約しつつ重要なデバイスを保護します。DoS プロテクション プロファイルを DoS プロテクション ポリシ#にアタッチします。ポリシ# ル#ルで、次のように設定します。
  - **Service**（サ#ビス）—保護中のサ#バ#上で使用中のサ#ビス（ポ#ト）を指定します。WEB サ#バ#を保護している場合は、HTTP、HTTPS、および WEB アプリケ#ションの他の適切なサ#ビス ポ#トを指定します。

    重要なサ#バ#の未使用のサ#ビス ポ#トについては、別の *DoS* 保護ポリシ#ル#ルを使用してください。
  - **Action**（アクション）—**Protect**（保護）を選#し、ル#ルの DoS 保護プロファイルを指定されたデバイスに適用します。保護は、DoS プロテクションを適用する唯一の アクションです。
  - ログ#送—管理を行いやすくするために、他の脅威ログとは別に直接管理者にメ#ルで、およびログ サ#バ#にDoS ログを#送します。
  - **Aggregate**（集約）—集約プロファイルを使用して重要なサ#バ#グル#プを保護します。
  - 分類化 > プロファイル—分類化プロファイルを使用し、個#の重要なサ#バ#を保護します。ハ#ドウェア ブロック テ#ブルを利用するには、分類化プロファイルを使用する必要があります。
  - 分類化 > アドレス—カウンタ#はファイアウォ#ルのリソ#スを消費します。分類化 DoS 保護プロファイルの場合、**source-IP-only**（送信元 **IP** のみ）、**destination-IP-only**（宛先 **IP** のみ）、あるいは#方（**src-dest-ip-both**（送信元#宛先 **IP** の#方））に#するマッチに基づき、接#がプロファイルのしきい値に加味されるかどうかを指定します。DoS 保護の目的、保護#象、保護するデバイスがインタ#ネットに接#されたゾ#ン#にあるかどうかに基づいて、しきい値カウンタ#の設定方法が異なります。

    ファイアウォ#ルは候補となるすべての IP アドレスに#してカウンタ#を保存することはできないため、インタ#ネットに接#されたゾ#ンでは**src-ip-only**（送信元 **IP** の

み）や**src-dest-ip-both**（送信元#宛先 **IP** の#方）を使用しないでください。境界ゾ#ンでは**destination-IP-only**（宛先 **IP** のみ）を使用します。

destination-IP-only（宛先 **IP** のみ）を使用すれば個#の重要なデバイスを保護できます。ポリシ#で指定した各デバイスが#理できる CPS レ#トより低い値の最大しきい値を設定します。

source-IP-only（送信元 **IP** のみ）および**Alarm**（アラ#ム）のしきい値を使用して疑わしいホストを監視します（インタ#ネットに接#されていないゾ#ン）。

ファイアウォ#ルは、**src-dest-ip-both**（送信元#宛先 **IP** の#方）のカウンタ#を追跡する方が、送信元 IP あるいは 宛先 IP のいずれかのカウンタ#を追跡する場合よりも多くのリソ#スを消費します。

ハ#ドウェアブロックテ#ブルをサポ#トするプラットフォ#ムでハ#ドウェアブロックテ#ブルを使用するには、***source-ip-only*** または***src-dest-ip-both*** のいずれかを使用する必要があります。 ***Destination-ip-only*** では、ソフトウェア テ#ブルを使用します。

STEP 3 | パケット バッファ保護をグロ#バルに有#にして、シングルセッション DoS 攻#、#一送信元 IP アドレスからの攻#からファイアウォ#ル バッファを保護し、組み合わせによってパケットバッファを消費する多#の小さなセッションを作成する送信元 IP アドレスからファイアウォ#ル バッファを保護します。

Global Packet Buffer Protection（グロ#バルパケットバッファ保護）は、ファイアウォ#ルを保護するための2フェ#ズのアプロ#チの最初のフェ#ズで、デフォルトで有#になっています。(手順 4 には、2 番目のフェ#ズであるゾ#ンごとのパケット バッファ保護が示されていますが、これも#定で有#になっています)。 グロ#バル パケット バッファ保護では、ファイアウォ#ル パケット バッファを消費するおそれのあるセッションや送信元 IP アドレスが個別に#出され、それらのセッションやパケットに RED が適用され、バッファの輻輳が#加すると、ドロップするパケット#が#やされます。

パケット バッファ保護の目的は、最初に RED を適用して問題のあるパケットをドロップし(グロ#バル保護)、攻#が#く場合は問題のあるセッションを破棄するか、問題のある送信元 IP アドレスをブロックして (セッションまたはホスト ブロッキング) (ゾ#ンごとの保護)、ファイアウォ#ルが高#延、高バッファ使用率の#態になり、その#態にとどまるのを防ぐことです。考え方としては、ソフトウェア レベルとハ#ドウェア レベルの#方でパケット バッ

ファを保護すると同時に、#延とパケット損失を削減し、問題のあるトラフィックを適切なタイミングで破棄するか、ブロックします。

パケット バッファ保護では、ファイアウォ#ルによって#理される大量のトラフィックがホストによって送信され、、セッションがセットアップされずに順次拒否される場合にも、ファイアウォ#ル バッファを保護します。このトラフィックの識別子は通常、同じ *6* タプルの識別子 (送信元 *IP* と宛先 *IP*、送信元と宛先ポ#ト、プロトコル、入力ゾ#ン) です。パケット バッファ保護を無#にすると、各パケットを#理して拒否するために必要なリソ#スによって、ファイアウォ#ルリソ#スが消費されます。

ゾ#ンごとのパケット バッファ保護が有#で、バッファ消費量が高レベルに達し、設定可能な時間持#する場合、ファイアウォ#ルでは問題のあるセッションまたはホストのみが破棄されます。ゾ#ンごとのパケット バッファ保護が無#の場合、ファイアウォ#ルでは RED が#行されますが、トラフィックの破棄やブロックは行われません。

- パケット バッファ使用率のベ#スラインの測定値から、ファイアウォ#ルのキャパシティを把握し、攻#を受けた場合にのみバッファ使用率が大幅に上昇するように、ファイアウォ#ルのサイズが適切に設定されていることを確認してください。通常のピ#ク時の動作時のパケット バッファの使用率と、どの時点で#延やドロップの問題が#生するかを把握します。ファイアウォ#ルのキャパシティが少なすぎて、標準のトラフィックでもバッファの使用にスパイクが#生する場合は、よりキャパシティの高いファイアウォ#ルが必要になります。

  PAN-OS 10.0 以降では、ベ#スラインのパケット バッファ使用率を把握し、攻#的な送信元を特定するために、 監視のみ モ#ド (デバイス > セットアップ > セッション > セッション設定) の使用を#討してください。監視のみ モ#ドでは、ファイアウォ#ルはパケット バッファの使用率を監視し、問題のあるセッションとソ#スについて警告しますが、それらをブロックしたりドロップしたりすることはありません。トレ#ドオフとして、トラフィックに影響を#えることなく、さまざまな アラ#ト および アクティベ#ト のしきい値を試して、結果を脅威ログで確認できますが、ファイアウォ#ルはパケット バッファ#攻#からは保護されません。#稼#トラフィックを非#稼#環境で複製できる場合は、アラ#ト および アクティベ#ト のしきい値を安全に試して、さまざまなしきい値設定でどのセッションにペナルティが課されるのか、またどのしきい値が正規のトラフィックに影響を及ぼし始めるのかを確認できます。

- バッファの使用#況、または CPU #理 (バッファ) の#延時間に基づいて、グロ#バル パケット バッファ保護のしきい値 (デバイス > セットアップ > セッション > セッション設定) を設定します。CPU #理#延に基づくパケット バッファ保護は、バッファの使用率から、バッファ保護よりも短時間にパケットの急激な大バ#ストに#答します。

  バッファ使用率を利用したパケット バッファ保護は、デフォルトで有#です:

  - アラ#ト—デフォルト値 (50%) で始めてパケット バッファの使用率を監視し、必要に#じてしきい値を調整します。
  - アクティベ#ト：デフォルトの アクティベ#ト しきい値は、PAN-OS 10.0 以降では 80%、PAN-OS 9.1 以前では 50% です。デフォルトを使用する代わりに、アクティブ化

のしきい値をベ#スライン使用量より 10 ~ 20% 高く設定して、パケット バッファ#の使用率を監視するのが最も安全です。パケット バッファ保護が時間#にアクティブになり、問題のあるセッションにペナルティを科すが通常の使用にはペナルティが課されない点まで、しきい値を調整します。

適切な アクティベ#ト 設定は環境と利用可能な#理リソ#スによって異なるため、通常は##が必要です。アクティベ#ト しきい値が低いほど、正規のトラフィックがブロックされる可能性が高くなりますが、攻#の#減がより早く開始されます。しきい値が高いほど、攻#の#減を開始するまでに時間がかかりますが、正規のトラフィックが影響を受ける可能性は低くなります。

アクティベ#ションのしきい値が環境に#して高すぎる場合、パケット バッファ保護がアクティブになる前に、正規のトラフィックに高負荷や#延の影響が#生します。

アクティベ#ションのしきい値が環境に#して低すぎる場合、トラフィックを#理するリソ#スがあるにもかかわらず、ファイアウォ#ルは不必要に多くの正#なパケットをドロップします。(これは、他のネットワ#クの問題がある場合にも#生する可能性があります。)

アクティベ#ションのしきい値が環境にほぼ適切であれば、正#なトラフィックがほとんどドロップされず、ファイアウォ#ル リソ#スに負荷がかかりません。ベ#スラインのパケット バッファ負荷を知ることが、しきい値を適切に調整するための鍵となります。たとえば、ピ#ク時間#にはパケット バッファ#の使用率がファイアウォ#ルの容量の 40 ~ 50% に急#する可能性があり、パケット バッファ#の使用率が 60 ~ 70% に達すると問題が#生することがわかっている場合は、 アクティベ#ト のしきい値を 55 ~ 60% に設定します。 。

PAN-OS 10.0 以降では、 アラ#ト および アクティベ#ト のしきい値を設定し、 モニタ#のみ モ#ドを使用して結果を表示することを##できます。監視のみ モ#ドでは、問題のあるトラフィックに#して何もアクションを#行しませんが、パケット バッファ保護をアクティブにする前に、しきい値がトラフィックにどのような影響を#えるかを確認できます。

パケット バッファの使用率を測定するには、Panorama Health Monitorを使用します。さらに、以下の CLI 操作コマンドも役立ちます。

- **> show running resource-monitor** コマンドは、CPU 統計を表示します。**ingress-backlogs** オプションは、オンチップ パケット記述子の少なくとも 2% を消費するセッションを表示します。
- パケット バッファ#保護がファイアウォ#ルをアクティブに保護しているセッションの場合、**> show session packet-buffer-protection** コマンドは、デ#タプレ#ン CPU リソ#スを最も多く消費するセッションを表示します。

パケット バッファ保護の#延ベ#スのアクティブ化は、デフォルトでは無#になっています。ファイアウォ#ルで拒否されるパケットが送信元から絶えず送信され、それによってリソ#スが消費される DoS 攻#は、#延ベ#スの保護では防ぐことはできません。ファイアウォ#ルでは、拒否されたトラフィックにセッションがセットアップされず、#延とはみな

されないためです。(ただし、バッファ使用率に基づくパケット バッファ保護では、これらのタイプの攻#を防防ぐことができます)。

レイテンシ#ベ#スのアクティベ#ション は、パケット バッファ#の使用率がまだ高くないときにオンチップ記述子の大量消費を#減し、パケット バッファ#が使い果たされる前にファイアウォ#ルに反#させたい場合に最適な方法です。

バッファの使用#況の割合ではなく、CPU#理の#延に基づく保護を有#にするには、#延ベ#スのアクティベ#ションを選#します。次の 3 つの設定では、使用率ベ#スのアラ#ト設定とアクティブ設定が置き換えられます。

- #延アラ#ト—デフォルト値 (50 ミリ秒) で始めて#延を監視し、必要に#じてしきい値を調整します。
- #延アクティベ#ト—デフォルト値 (200 ミリ秒) で始めて#延を監視し、必要に#じてしきい値を調整します。
- #延最大許容値—デフォルト値 (500 ミリ秒) で始めて#延を監視し、必要に#じてしきい値を調整します。トラフィックが#延アクティベ#トのしきい値に達すると、ファイアウォ#ルでは RED でトラフィックのドロップが開始され、#延が#延最大許容範#に達するまで、ドロップ レ#トが#加します。#延最大許容値では、ドロップ レ#トの確率は 100% 近くになります。

各ファイアウォ#ルの#延を測定します。

- ***fw-1> debug dataplane pow performance \| match pbp*** 運用コマンド。
- デ#タプレ#ン負荷が高いときにロギングを有#にして、通知を受信し、ログ情報を表示します (デバイス > セットアップ > 管理 > ロギングとレポ#ト 、および高 ***DP*** 負荷でログオンを有#化)。運用 *CLI* コマンド#行中のリソ#ス モニタ#を表示して、デ#タプレ#ン負荷を確認します。また、テクニカル サポ#ト ファイルを作成し、デ#タプレ#ン ログをテキスト形式で確認することもできます。

- しきい値とタイマ# (デバイス > セットアップ > セッション > セッション設定) を設定して、問題のあるセッションを破棄するタイミングや、問題のある送信元 IP アドレスをブロックするタイミングを定義します。ファイアウォ#ルでは、ゾ#ン別パケット バッファ保護を有#にした場合にのみ、これらのしきい値とタイマ#が使用されます。グロ#バル パケット バッファ保護のみを有#にすると、ファイアウォ#ルではトラフィックに#して RED が#行されますが、トラフィックの破棄やブロックは行われません。

  設定値は、ファ使用率のエクスペリエンスと測定、バッファ輻輳による#延とパケット ドロップの許容度、そしてネットワ#クとそのユ#ザ#に影響を#える#延とパケット バッファ消費を回避するためにトラフィックをどの程度積極的にドロップするかに基づいて設定します。

  - ブロック カウントダウンしきい値—問題のあるトラフィックを破棄するか、ブロックするためのカウントダウンを開始するバッファ使用率または#延しきい値 (ミリ秒 #位)。バッファの輻輳または#延がブロック カウントダウンしきい値しきい値に達す

る と、ブロック ホ#ルド タイムが減少し始めます。(ブロック保持時間が#過すると、ファイアウォ#ルはセッションを破棄するか、問題のあるホストをブロックします。)

ブロック カウントダウンしきい値をアクティベ#トまたは#延アクティベ#トしきい値より 10% 低く設定して、パケット バッファ使用率 を監視し、必要に#じて値を調整します。 この方法では、デフォルト設定 (#延の場合は 80% または 500ms) よりも短い時間で、問題のある IPアドレスがブロックされます。ブロック保持時間 の値が低いほど、ファイアウォ#ルはセッションを破棄したり、問題のある送信元 IP をブロックしたりして、早めにバッファ#の輻輳を緩和し始めます。値が大きいほど、ファイアウォ#ルによって#減されるまで攻#が##できる時間が長くなります。

- ブロック ホ#ルド タイム—ファイアウォ#ルによってセッションが破棄されるか、送信元 IP アドレスがブロックするまでに、問題のあるセッションがブロック カウントダウンしきい値を超えた#態を維持できる時間。値が低いほど、ファイアウォ#ルはより早くパケット バッファ保護をアクティブにし、ハ#ドウェア ブロック テ#ブル やソフトウェア ブロック テ#ブル (どちらもハ#ドウェア ブロック テ#ブルを持つシステム上) を利用してパケット バッファ#を保護します。

  値 30 秒から始めてパケット バッファ使用率を監視し、必要に#じて時間を調整します。この方法では、デフォルト設定 (60秒) より短い時間で、速く問題のある IP アドレスがブロックされます。時間の値が大きいほど、ファイアウォ#ルによって#減されるまで攻#が##できる時間が長くなります。

  ブロック ホ#ルド タイムは、輻輳がブロック カウントダウンしきい値を超えている限り減少します。ブロック ホ#ルド タイムが 0 になると、ファイアウォ#ルによってセッションは破棄されるか、送信元 IP アドレスがブロックされます。

- ブロック期間—ブロック ホ#ルド タイムが過ぎて、 送信元 IP アドレスが隔離 (ブロック) される時間。デフォルト値 (3600 秒) で始めます。送信元 IP アドレスを 1 時間ブロックすると業務上のペナルティが大きすぎる場合は、値を減らします。パケット バッファの使用率を監視し、必要な場合は値を調整します。

パケット バッファしきい値の設定方法は、ネットワ#ク トラフィックとそのトラフィックの#理方法によって異なります。

- デフォルト設定は控えめに設定されており、セッションの破棄や、送信元 IPアドレスのブロックまでの、パケット バッファの輻輳の##時間は長くなっています。輻輳の期間中、ファイアウォ#ルでは、潜在的に正#なセッションと送信元はそれほど迅速にブロックされませんが、これにはパケット バッファの輻輳を引き起こしていない正#なセッションの速度が低下するという潜在的なコストがかかります。これが、より低く、より積極的なしきい値から始めるというベスト プラクティスの存在理由です。
- ネットワ#クの速度低下に#するユ#ザ#の苦情は、パケット バッファのしきい値が控えめすぎることを示している可能性があります。これらの苦情に##するには、アクティベ#トレ#トとブロック カウントダウンしきい値を下げ て、RED パケットドロップを早く開始します。ブロック ホ#ルド タイムを縮めて、バッファ消費率がブロック カウントダウン

しきい値に達してから、ファイアウォ#ルによって IP アドレスのブロックまたはセッションの破棄が開始するまでの時間を短縮します。

問題のあるトラフィックの破棄またはブロックまでの時間を短縮すると、パケット バッファ消費の問題を引き起こしていない正#なトラフィックが、問題のあるトラフィックによる#延やパケット ドロップの問題の影響を受けずに問題のあるトラフィックを隔離することができます。ただし、大量のトラフィックを送信する正#なセッションや送信元 IP アドレスが隔離されるまでの時間も短くなるおそれがあります。

- アクティベ#ト レ#トとブロック カウントダウンしきい値を低く設定すると、DNS やその他の主要インフラストラクチャ トラフィックなどの主要正#なトラフィックがブロックされるおそれがある場合は、ブロック ホ#ルド タイムの値を高く設定して、隔離アクションを#らせ、パケット バッファの使用#況を#察してください。
- #延とパケット損失に#する、ネットワ#クにとって有意義なセッションを破棄するタイミングや、送信元 IP アドレスのブロックするタイミングとのバランスは、パケット バッファ保護のしきい値を調整して#現します。

STEP 4 | パケット バッファ保護の第 2 フェ#ズでは、入力ゾ#ンごとにファイアウォ#ル バッファが保護されます。この保護機能は、PAN-OS 10.0 以降ではデフォルトで有#ですが (PAN-OS 9.1 以前ではデフォルトで無#です)、この保護機能を利用するには、グロ#バル パケット バッファ保護も有#にする必要があります。そうしないとゾ#ンごとのパケット バッファ保護は機能しません。ゾ#ンごとのパケット バッファ保護では、問題のあるセッションが破

棄され、問題のある送信元 IP アドレスがブロックされます。この保護機能は、特定の入力ゾ#ンに追加の保護レイヤが必要なときのベスト プラクティスです。

特定のゾ#ンの送信元 *IP* アドレスのブロックや、セッションの破棄を行わないときは、ゾ#ンごとのパケット バッファ保護を無#にします (デフォルトでは、ファイアウォ#ルによって *RED* もグロ#バルに適用されるため、パケット バッファには引き#きプライマリ保護レイヤが適用されます)。送信元 *IP* アドレスをブロックすると、問題のあるセッションだけではなく、そのアドレス#のすべてのトラフィックがブロックされます。ソ#ス*IP*アドレスが*NAT*デバイスの場合、*NAT*デバイスの背後で#生する大量のユ#ザ#フロ#が存在している可能性があります。

- ゾ#ンごとの保護の無#と有#を切り替えるには、ネットワ#ク > ゾ#ンをクリックし、#存のゾ#ンを選#するか 、ゾ#ンを追加して 、パケット バッファ保護を有#化の選#と選#解除を切り替えます。

ゾ#ンごとのパケット バッファ保護の有#と無#の切り替え#討するときは、外部からの攻#に脆弱なゾ#ンだけでなく、#部ネットワ#クについても考慮してください。潜在的な#部脅威、#部デバイスの設定ミス、大量の不正トラフィックを生成する *NIC* アダプタ#の障害、ファイアウォ#ルの設定ミスを考慮してください。

ファイアウォ#ルでは、一意の *6* タプル識別子 (送信元と宛先*IP*、送信元と宛先のポ#ト、プロトコル、入力ゾ#ン) によってすべての主要トラフィック送信元が識別されるため、以上のような不具合があると、ファイアウォ#ルに大量のトラフィックを送信する正#な送信元からのトラフィックが拒否されるおそれがあります。パケット バッファの輻輳期間中は、問題のある送信元とともに大量のトラフィックを送信する正#な送信元にも *RED* による影響が生じます。

STEP 5 | ベストプラクティスの脆弱性保護プロファイルをすべてのセキュリティポリシ#許可ル#ルに付#します。

境界における#用の大容量 DDoS 保護中、ゾ#ン プロテクション プロファイル、DoS 保護プロファイル、および許可するトラフィックのポリシ#ル#ル、パケット バッファ保護、脆弱性保護を組み合わせることで、ネットワ#クや最も重要なリソ#スに#して複#の DoS 保護層を適用できます。

デプロイ後の DoS およびゾ#ン プロテクションのベストプラクティスに#う

ゾ#ンおよび DoS 保護のデプロイ後にすべてが計#通りに機能していることを確認し、ネットワ#クが#大するのに合わせて、すべてが機能していることを確認するための作業を行います。

STEP 1 | ファイアウォ#ルのパフォ#マンスを計測し、許容できる範#に#まっていることを確認しつつ、ゾ#ンおよび DoS 保護がファイアウォ#ル リソ#スに#える影響を把握します。

ゾ#ンおよび DoS 保護の水準（復#化など、リソ#スを消費する他の機能を含める）が高くファイアウォ#ル リソ#スを消費しすぎる場合、セキュリティを妥協するのではなく、リソ#スをスケ#ルアップすることがベストプラクティスになります。

STEP 2 | ログ#送を設定します。

管理を行いやすくするために、別のログ#送プロファイルを使用して他の脅威ログとは別けて DoS およびゾ#ンのしきい値イベント ログを#送します。DoS およびゾ#ン ログを#連する管理者にメ#ルで、およびログ サ#バ#に送信するため、通知には DoS 攻#を示唆するイベントだけを含めます。DoS 保護ポリシ#ル#ル（**Policies**（ポリシ#） > **DoS Protection**（**DoS** 保護））で DoS イベント ログ#送を、各ゾ#ン（**Network**（ネットワ#ク） > **Zones**（ゾ#ン））でゾ#ン イベント ログ#送を設定します。

Alarm Rate（アラ#ム レ#ト）のしきい値イベント ログ メッセ#ジを低か通知の重大度に設定します。DoS 保護の**Activate**（アクティベ#ト）、**Maximum**（最大）およびゾ#ン プロテクションの**Activate Rate**（アクティベ#ト レ#ト）、**Max Rate**（最大レ#ト）のしきい値イベント ログ メッセ#ジを重要の重大度に設定します。フラッドのしきい値を適切に設定したら、脅威や異常なイベントだけが表示されるため、ネットワ#ク上のフラッド攻#の可能性をログで確認できるようになります。誤ったアラ#トが多く表示される場合は、しきい値が小さすぎるか、ファイアウォ#ルのサイズが##するトラフィックと合っていません。

ログ サ#バ#を#倒しないよう、ログの大きさを管理できる程度に抑えてファイアウォ#ル リソ#スを節約するために、ファイアウォ#ルは *10* 秒#にログを蓄積します。

STEP 3 | DoS 攻#の他の兆候がないか、調査してください。

フラッドのしきい値を超過した際に管理者が通知を受け取れるようにログ#送を設定するだけでなく、攻#の兆候をチェックして DoS 攻#の可能性がないか調査します：

- DoS 脅威アクティビティを確認（**ACC** > **Threat Activity**（脅威アクティビティ））し、攻#パタ#ンを探します。
- この機能をサポ#トしているファイアウォ#ル モデル（PA-3050、PA-3060、PA-3200 シリ#ズ、PA-5200 シリ#ズおよびPA-7000 シリ#ズ）の場合、DoS 攻#の可能性のあるため、ファイアウォ#ルがブロックした IP アドレスについて、ブロックされた IP アドレスの監視（**Monitor**（監視） > **Block IP List**（ブロック **IP** リスト））を行います。**Block**

Source（ブロック ソ#ス）列は、IP アドレスをブロックした分類化 DoS 保護プロファイルの名前を特定します。

- ファイアウォ#ル上でのトラフィックの部分的あるいは完全な停止、ウェブ ブラウジングやエンドポイントの接#の#延、新規セッションの失敗は、DoS 攻#の可能性を示唆します。高い CPU 使用率、パケット バッファおよびディスクリプタの枯#、アクティブなセッション#の急#も、DoS 攻#の可能性を示唆します。
- DoS アクティビティを監視するためのゾ#ンおよび DoS 保護のイベント ログとグロ#バル カウンタ#の詳細を確認してください。

フラッドしきい値違反は、*DoS* 攻#を示している可能性がありますが、*CPS* 値の設定ミス、別の#部デバイスの設定ミス、*NIC* アダプタ#の障害、#部#係者からの潜在的な脅威、または不適切なファイアウォ#ル サイズ設定を示している可能性もあります。

STEP 4 | ネットワ#クのトラフィック パタ#ンは時と共に#化し、ネットワ#クに新規デバイスが追加されたり、古いデバイスが削除されたり、特別なイベントが一時的にトラフィック パタ#ンに影響を#えたりすることもあります。

これらの理由により、定期的にCPSの再測定を行い、ゾ#ンおよび DoS フラッドのしきい値設定を見直してください（ネットワ#クは常に進化しているため、DoS およびゾ#ン プロテクションにはこのような繰り返しアプロ#チが求められます）。