目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[レートリミット ICMP/Smurf](#)
[レートリミット TCP Syn パケット](#)
[11.1(X)CC](#)
[12.0(X)[S/T/M]](#)
[CAR の FAQ](#)
[値を CAR のために使用するために識別する方法レートリミット Syn パケットに支配しますか。](#)
[過剰な Syn パケットを制限するかどうかどのようにしてわかりますか。](#)
[GSR で CAR を有効にできますか?](#)
[Cisco 7500 で分散CAR (dCAR) を有効にできるか](#)
[Cisco 7200 で CAR を有効にできるか](#)
[その他の機能および選択肢](#)
[IP Receive ACL機能](#)
[IPソース トラッカー](#)
[関連情報](#)

概要

ネットワークでは、通常のネットワーク トラフィックとともにサービス拒否（DoS）攻撃パケットのストリームを受信することがあります。 ネットワークがアップのままになっているようにそのような状況で、「ネットワークパフォーマンスが低下するように制限する」と比率呼ばれるメカニズムを使用できます。 これらの方式によって制限する比率を実現させるのに Cisco IOS ® ソフトウェアを使用できます:

- 専用アクセス レート（CAR）
- トラフィック シェーピング
- モジュラー Quality of Service コマンド ライン インターフェイス（QoS CLI）によるシェーピング および ポリシング

この資料は DoS攻撃で使用のための CAR を説明します。 他の方式は基本概念のちょうどバリアントです。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアおよびハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 11.1 CC および 12.0 T
- CAR

- Cisco IOS ソフトウェア Release 11.2 と それ以降、トラフィック シェーピングをサポートする。
- Cisco IOS ソフトウェア リリース 12.0XE、12.1E、Modular QoS CLI をサポートする 12.1T。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

レートリミット ICMP/Smurf

これらの access-list を設定して下さい:

CAR を有効に するために、ボックスの Cisco Express Forwarding （ CEF ）を有効に して下さい。 さらに、CAR のための CEF スイッチのインターフェイスを設定して下さい。

DS3 の出力例使用帯域幅の値は帯域幅を入力します。 トラフィックの特定の種類を制限したいと思う比率およびインターフェイス 帯域幅に基づいて値を選択して下さい。 より小さい入力 インターフェイスの場合、低いレートを設定できます。

レートリミット TCP Syn パケット

11.1(X)CC

どのホストが攻撃の下にあるか確認したら、これらのアクセス リストを設定して下さい:

注この例では、攻撃の下のホストは 10.0.0.1 です。

どのホストが DoS攻撃の下に、およびあるかネットワークを保護したいと思ったら知らない場合これらのアクセス リストを設定して下さい:

注すべての TCP Syn パケットのための 64000 ビット/秒へのレートリミット。

12.0(X)[S/T/M]

どのホストが攻撃の下にあるか確認したら、これらのアクセス リストを設定して下さい:

注この例では、10.0.0.1 は攻撃の下にホストです。

ホストが攻撃の下に、およびである確実ネットワークを保護したいと思ったらではない場合これらのアクセス リストを設定して下さい:

注すべての TCP Syn パケットのための 64000 ビット/秒へのレートリミット。

CAR の FAQ

値をレートリミット Syn パケットに CAR ルールのために使用するために識別する方法か。

運用しているネットワークについて理解してください。 トラフィック の 種類は一定のデータのためのアクティブな TCP セッションの数を判別します。

- WWW のトラフィックでは、FTP サーバ ファームのトラフィックよりもかなり高い比率で TCP Syn パケットが混合しています。
- PC クライアントのスタックは、少なくとも他のすべての TCP パケットに対して ACK (確認応答) する傾向があります。 他のスタックはより頻繁により少しをまたは確認できます。
- 家庭 ユーザ エッジのまたはカスタマー ネットワーク エッジのこれらの CAR ルールを適用する必要があるかどうか確認して下さい。

WWW に関しては、トラフィック ミックスはここにあります:

Webファームからダウンロードする各 5k ファイルに関しては、Webファームはここに示されているように 560 バイトを、受け取ります:

- 80 バイト [SYN、ACK]
- 400 バイト [320 バイトの HTTP 構造、2 ACK]
- 80 バイト [FIN、ACK]

と Webファームからの出トラフィックと Webファーム is10:1 からの入トラフィック間の比率仮定して下さい。 Syn パケットを構成するトラフィック量は 120:1 です。

OC3 リンクがある場合、155 mbps/120 == 1.3 mbps に TCP Syn パケット 比率を制限します。

Webファーム ルータの入力 インターフェイスで、設定して下さい:

TCP 同期信号 パケット 比率はより長くより小さく得る TCP セッションの長さはなります。

MP3 ファイルは平均の 4 つから 5 つの mgbps でありがちです。 4 mgbps ファイルのダウンロードは 3160 バイトに入トラフィックをその量生成します:

- 80 バイト [SYN、ACK]
- 3000 バイト [ACK + FTP get]
- 80 バイト [FIN、ACK]

出トラフィックに対する TCP SYN のレートは、155mbps / 120000 == 1.3kbps です。

設定例:

過剰な Syn パケットを制限するかどうか確認する方法

サーバの通常接続速度を知っている場合、CAR を有効に する前後に図を比較できます。 比較は接続速度のドロップするの発生を識別するのを助けます。 比率のドロップするを見つける場合、割り当てに CAR パラメータをより多くのセッション増分して下さい。

ユーザが TCP セッションを容易に設定できるかどうか確認して下さい。 CAR 制限が余りにも制限する場合、TCP セッションを設定する倍数試みを試みるにはユーザーのニーズ。

GSR で CAR を有効にできますか?

はい。 エンジン 0 およびエンジン 1 ラインカードは CAR をサポートします。 Cisco IOS ソフトウェア リリース 11.2(14)gs2 およびそれ以降は CAR サポートを提供します。 CAR のパフォーマンス影響は CAR の数によって支配します適用します決まります。

また、エンジン 1 のラインカードの方が、エンジン 0 のラインカードよりパフォーマンス上の影響は大きくなります。 0 ラインカード エンジンの CAR を有効に したいと思う場合、Cisco バグ ID CSCdp80432 （登録ユーザのみ）に気づく必要があります。 レート制限 マルチキャストトラフィックに CAR を有効に したいと思う場合 Cisco バグ ID CSCdp32913 （登録ユーザのみ）が影響を与えないようにして下さい。 Cisco バグ ID CSCdm56071 （登録ユーザのみ）は CAR を有効に する前に認識しているを必要があるもう一つの不具合です。

Cisco 7500 で分散CAR (dCAR) を有効にできるか

はい、Cisco IOS ソフトウェア リリース 11.1(20)cc の RSP/VIP プラットフォームサポート dCAR、およびすべての 12.0 ソフトウェア リリース。

CAR はパフォーマンスにある程度影響を与えます。 CAR構成に基づいて、OC3 の VIP2-50 の行比率を[インターネットのためにトラフィックを混合して下さい] [dCAR を通して]実現できます。 Cisco バグ ID CSCdm56071 （登録ユーザのみ）が影響を与えないようにして下さい。 CARの出力を使用したいと思う場合 Cisco バグ ID CSCdp52926 （登録ユーザのみ）は接続に影響を与える場合があります。 dCAR を有効に する場合、Cisco バグ ID により CSCdp58615 （登録ユーザのみ） VIPクラッシュを引き起こす場合があります。

Cisco 7200 で CAR を有効にできるか

はい。 NPE は Cisco IOS ソフトウェア リリース 11.1(20)cc の CAR、および 12.0 ソフトウェア リリースをすべてサポートします。

CAR は CAR構成に基づいてパフォーマンスに、ある程度影響を与えます。 これらのバグのための修正を得て下さい: Cisco バグ ID CSCdm85458 （登録ユーザのみ）および Cisco バグ ID CSCdm56071 （登録ユーザのみ）。

注インターフェース/サブインターフェースの多数の CAR エントリは一致する「CAR」文を見つけるためにルータが CAR 文のライナー サーチを行う必要があるのでパフォーマンスを低下させます。

その他の機能および選択肢

IP Receive ACL機能

Cisco IOS software release 12.0(22)S は Cisco 12000 シリーズ インターネット ルータの IP Receive ACL 機能 機能があります。

IP Receive ACL 機能 機能はルータに達するために送信されるトラフィックに基本的なフィルタを提供します。 ルータは攻撃から機能が入力 インターフェイスのすべての入力 Access Control List （ ACL ）をフィルタリングするので高優先順位 ルーティングプロトコルトラフィックを保護できます。 IP Receive ACL 機能 機能はルートプロセッサがパケットを受信する前に分散ラインカードのトラフィックをフィルタリングします。 この機能はユーザがルータに対してサービス拒

否（DoS）フラッドをフィルタリングすることを可能にします。 従って、この機能はルートプロセッサのパフォーマンス低下を防ぎます。

IP レシーブ APL を詳細については参照して下さい。

IPソース トラッカー

Cisco IOS ソフトウェア リリース 12.0(21)S は Cisco 12000 シリーズ インターネット ルータの IP ソース トラッカー 機能をサポートします。 Cisco IOS software release 12.0(22)S は Cisco 7500 シリーズ ルータのこの機能をサポートします。

IP ソース トラッカー 機能は攻撃の下にある疑うホストへのフローそのトラフィックについての情報を収集することを可能にします。 この機能はまた容易にネットワークのエントリポイントに戻って攻撃をトレースすることを可能にします。 この機能を通してネットワークイングレスポイントを特定するとき、攻撃を効果的にブロックするのに ACL か CAR を使用できます。

詳細については IP ソース トラッカーを参照して下さい。

関連情報

- Nimda ウイルスからネットワークを保護する方法
- IP レシーブ APL
- IPソース トラッカー
- テクニカルサポートとドキュメント - Cisco Systems