

Using CAR During DOS Attacks

Document ID: 12764

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Rate Limit ICMP/Smurf

Rate Limit TCP SYN Packets

- 11.1(X)CC
- 12.0(X)[S/T/M]

CAR Frequently Asked Questions

- How to Identify the Values to Use for the CAR Rules to Rate Limit SYN Packets?
- How Do I Know if I Restrict too Many SYN Packets?
- Can I Enable CAR on a Gigabit Switch Router (GSR)?
- Can I Enable Distributed CAR (dCAR) on a Cisco 7500?
- Can I Enable CAR on a Cisco 7200?

Other Features and Alternatives

- IP Receive ACL
- IP Source Tracker

Related Information

Introduction

Sometimes, a network receives a stream of Denial of Service (DoS) attack packets along with the regular network traffic. In such situations, you can use a mechanism called "rate limiting" in order to allow the network performance to degrade, so that the network remains up. You can use Cisco IOS[®] software to achieve rate limiting through these schemes:

- Committed Access Rate (CAR)
- Traffic Shaping
- Shaping and Policing through Modular Quality of Service Command Line Interface (QoS CLI)

This document discusses CAR for use in DoS attacks. The other schemes are just variants of the basic concept.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 11.1CC and 12.0 mainline, which support CAR.
- Cisco IOS Software Release 11.2 and later, which support Traffic Shaping.

- Cisco IOS Software Releases 12.0XE, 12.1E, 12.1T, which support Modular QoS CLI.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Rate Limit ICMP/Smurf

Configure these access-lists:

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply

interface <interface> <interface #>
  rate-limit input access-group 102 256000 8000 8000 conform-action transmit
  exceed-action drop
```

In order to enable CAR, you must enable Cisco Express Forwarding (CEF) on the box. In addition, you must configure a CEF-switched interface for CAR.

The sample output uses bandwidth values for DS3 type bandwidths. Choose values based on the interface bandwidth and the rate at which you want to limit a particular type of traffic. For smaller ingress interfaces, you can configure lower rates.

Rate Limit TCP SYN Packets

11.1(X)CC

If you know which host is under attack, configure these access lists:

```
access-list 103 deny tcp any host 10.0.0.1 established

!--- Let sessions in progress run.

access-list 103 permit tcp any host 10.0.0.1

!--- Rate limit the initial TCP SYN packet, because the other packets
!--- in the TCP session would have hit the earlier entry in the ACL.

interface <interface> <interface #>
  rate-limit input access-group 103 8000 8000 8000 conform-action transmit
  exceed-action drop
```

Note: In this example, the host under attack is 10.0.0.1.

If you do not know which host is under DoS attack, and you want to protect a network, configure these access lists:

```
access-list 104 deny tcp any any established

!--- Let sessions in progress run.
```

```

access-list 104 permit tcp any any

!--- Rate limit the initial TCP SYN packet, because the other packets
!--- in the TCP session would have hit the earlier entry in the ACL.

interface <interface> <interface #>
  rate-limit input access-group 104 64000 8000 8000 conform-action transmit
  exceed-action drop

```

Note: Rate limit to 64000 bps for all TCP SYN packets.

12.0(X)[S/T/M]

If you know which host is under attack, configure these access lists:

```

access-list 105 permit tcp any host 10.0.0.1 syn

!--- Remember that your interest lies in syn packets only.

interface <interface> <interface #>
  rate-limit input access-group 105 8000 8000 8000 conform-action transmit
  exceed-action drop

```

Note: In this example, 10.0.0.1 is the host under attack.

If you are not sure which host is under attack, and you want to protect a network, configure these access lists:

```

access-list 106 permit tcp any any syn

!--- Remember that your interest lies in syn packets only.

interface <interface> <interface #>
  rate-limit input access-group 106 64000 8000 8000 conform-action transmit
  exceed-action drop

```

Note: Rate limit to 64000 bps for all TCP SYN packets.

CAR Frequently Asked Questions

How to Identify the Values to Use for the CAR Rules to Rate Limit SYN Packets?

Understand your network. The type of traffic determines the number of active TCP sessions for a fixed amount of data.

- WWW traffic has a much higher mix of TCP SYN packets than FTP server farm traffic.
- PC client stacks tend to acknowledge at least every other TCP packet. Other stacks can acknowledge less or more often.
- Check whether you need to apply these CAR rules on the residential user edge or at the Customer Network edge.

```

users ---- { ISP } --- web farm

```

For WWW, here is the traffic mix:

For every 5k file that you download from the web farm, the web farm receives 560 bytes, as shown here:

- 80 bytes [SYN, ACK]
- 400 bytes [320 byte HTTP structure, 2 ACKs]
- 80 bytes [FIN, ACK]

Assume that the ratio between egress traffic from the web farm and ingress traffic from the web farm is 10:1. The amount of traffic that makes up SYN packets is 120:1.

If you have an OC3 Link, you limit the TCP SYN packets rate to $155 \text{ mbps} / 120 = 1.3 \text{ mbps}$.

On the ingress interface at the web farm router, configure:

```
rate-limit input access-group 105 1300000 256000 256000 conform-action transmit
exceed-action drop
```

The TCP SYN packet rate gets smaller as the length of your TCP sessions get longer.

```
users ---- { ISP } --- MP3/FTP Farm
```

MP3 files tend to be 4 to 5 mgbps in size on an average. Download of a 4 mgbps file generates ingress traffic that amounts to 3160 bytes:

- 80 bytes [SYN, ACK]
- 3000 bytes [ACKs + FTP get]
- 80 bytes [FIN, ACK]

The rate of TCP SYNs to egress traffic is $155 \text{ mbps} / 120000 = 1.3 \text{ kbps}$.

Configure:

```
rate-limit input access-group 105 1300 1200 1200 conform-action transmit
exceed-action drop
```

How Do I Know if I Restrict too Many SYN Packets?

If you know your usual connection rate on your servers, you can compare the figures before and after you enable CAR. The comparison helps you identify the occurrence of a drop in your connection rate. If you find a drop in the rate, increment your CAR parameters to permit more sessions.

Check whether users are able to establish TCP sessions easily. If your CAR limits are too restrictive, users need to make multiple attempts to establish a TCP session.

Can I Enable CAR on a Gigabit Switch Router (GSR)?

Yes. Engine 0 and Engine 1 line cards support CAR. Cisco IOS Software Release 11.2(14)GS2 and later provide CAR support. The performance impact of CAR depends on the number of CAR rules you apply.

The performance impact is also greater on Engine 1 line cards than on Engine 0 line cards. If you want to enable CAR on Engine 0 line cards, you must be aware of Cisco bug ID CSCdp80432 (registered customers only) . If you want to enable CAR to rate-limit multicast traffic, ensure that Cisco bug ID CSCdp32913 (registered customers only) does not affect you. Cisco bug ID CSCdm56071 (registered customers only) is another bug you must be aware of before you enable CAR.

Can I Enable Distributed CAR (dCAR) on a Cisco 7500?

Yes, the RSP/VIP platform supports dCAR in Cisco IOS Software Release 11.1(20)CC, and all 12.0 Software Releases.

CAR impacts performance to some extent. Based on the CAR configuration, you can achieve line rate [for Internet Mix traffic] with a VIP2–50 [through dCAR] on an OC3. Ensure that Cisco bug ID CSCdm56071 (registered customers only) does not affect you. If you want to use output CAR, Cisco bug ID CSCdp52926 (registered customers only) can affect your connectivity. If you enable dCAR, Cisco bug ID CSCdp58615 (registered customers only) can cause a VIP crash.

Can I Enable CAR on a Cisco 7200?

Yes. The NPE supports CAR in Cisco IOS Software Release 11.1(20)CC, and all 12.0 Software Releases.

CAR impacts performance to some extent, based on the CAR configuration. Get fixes for these bugs: Cisco bug ID CSCdm85458 (registered customers only) and Cisco bug ID CSCdm56071 (registered customers only) .

Note: A large number of CAR entries in an interface/sub-interface degrades performance because the router needs to perform a linear search on the CAR statements to find the "CAR" statement that matches.

Other Features and Alternatives

IP Receive ACL

Cisco IOS Software Release 12.0(22)S contains the IP Receive ACL feature on the Cisco 12000 Series Internet Router.

The IP Receive ACL feature provides basic filters for traffic destined to reach the router. The router can protect high-priority routing protocol traffic from an attack because the feature filters all input access control list (ACL) on the ingress interface. The IP Receive ACL feature filters traffic on the distributed line cards before the route processor receives packets. This feature allows users to filter Denial of Service (DoS) floods against the router. Therefore, this feature prevents performance degradation of the route processor.

Refer to IP Receive APL for more details.

IP Source Tracker

Cisco IOS Software Release 12.0(21)S supports the IP Source Tracker feature on the Cisco 12000 Series Internet Router. Cisco IOS Software Release 12.0(22)S supports this feature on the Cisco 7500 Series Router.

The IP Source Tracker feature allows you to gather information about the traffic that flows to a host that you suspect is under attack. This feature also allows you to easily trace an attack back to the entry point in the network. When you identify the network ingress point through this feature, you can use ACLs or CAR to block the attack effectively.

Refer to IP Source Tracker for more information.

Related Information

- [How to Protect Your Network Against the Nimda Virus](#)
 - [IP Receive APL](#)
 - [IP Source Tracker](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 06, 2008

Document ID: 12764
