

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[速率限制ICMP/Smurf](#)

[速率限制TCP SYN数据包](#)

[11.1\(X\)CC](#)

[12.0\(X\)\[S/T/M\]](#)

[CAR 常见问题](#)

[如何识别值使用CAR规定到速率限制SYN数据包？](#)

[如何知道我是否限制过多的SYN数据包？](#)

[能否在千兆交换路由器 \(GSR\) 上启用 CAR？](#)

[能否在 Cisco 7500 上启用分布式 CAR \(dCAR\)？](#)

[能否在 Cisco 7200 上启用 CAR？](#)

[其他特性和选择](#)

[IP 接收 ACL](#)

[IP 源跟踪器](#)

[相关信息](#)

简介

有时，网络与正常网络流量一起接收服务拒绝(DoS)攻击数据包数据流。在这些情况下，您能使用呼叫“限制的速率的机制”为了允许网络性能降低，因此网络依然是。您能使用Cisco IOS软件达到限制通过这些机制的速率：

- 承诺接入速率 (CAR)
- 流量整形
- 整形和策略通过模块化服务质量命令行界面(服务质量命令行接口)

本文在DOS攻击讨论CAR为使用。其他机制是基本概念的变形。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS软件版本11.1cc及12.0主线，支持[CAR](#)。
- Cisco IOS软件版本11.2及以上版本，支持[流量整形](#)。
- Cisco IOS软件版本12.0XE， 12.1E， 12.1T，支持[模块化QoS CLI](#)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[速率限制ICMP/Smurf](#)

配置这些访问列表：

为了启用CAR，您必须启用在方框的思科快速转发(CEF)。另外，您必须配置CAR的一个经过CEF交换的接口。

DS3的输出示例:用途带宽值键入带宽。选择根据您要限制流量特定类型的接口带宽和速率的值。对于更加小的入口接口，您能配置更低的速率。

[速率限制TCP SYN数据包](#)

[11.1\(X\)CC](#)

如果知道哪台主机受到攻击，请配置这些访问列表：

注意： 在本例中，在攻击下的主机是10.0.0.1。

如果不知道哪台主机受到DOS攻击，并且您要保护网络，请配置这些访问列表：

注意： 对64000位/秒的速率限制所有TCP SYN数据包的。

[12.0\(X\)\[S/T/M\]](#)

如果知道哪台主机受到攻击，请配置这些访问列表：

注意： 在本例中，10.0.0.1受到主机攻击。

如果主机受到攻击，并且不是肯定的您要保护网络，请配置这些访问列表：

注意： 对64000位/秒的速率限制所有TCP SYN数据包的。

[CAR 常见问题](#)

[如何识别值使用CAR规则到速率限制SYN数据包？](#)

了解您的网络。流量类型确定活动TCP会话数量一定量的数据的。

- WWW数据流比FTP服务器群数据流有更高的TCP同步信息包混合。
- 全双工流量控制堆叠倾向于确认至少其他TCP数据包。其他堆叠能经常确认较少或。
- 证实您是否需要运用这些CAR规则在住宅用户边缘或在用户网络边缘。

对于WWW，这是流量混合：

对于您从Web区域下载每个5k文件，Web区域接收560个字节，如显示此处：

- 80字节[SYN，ACK]
- 400个字节[320字节HTTP结构，2ACK]
- 80字节[FIN，ACK]

假设，在出口流量从Web区域和入口流量之间的比率从Web区域是10:1。组成SYN数据包的流量总量是120:1。

如果有一条OC3链路，您对155 mbps/120 == 1.3 mbps限制TCP SYN数据包速率。

在Web区域路由器的入口接口，请配置：

TCP Syn信息包速率变得更加小，虽然长度您的TCP会话变得更加长。

MP3文件在大小上倾向于是4到5 mgbps在平均值。4 mgbps文件的下载生成入口流量该总数对3160个字节：

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

速率对出口流量的TCP SYN是155 mbps/120000 == 1.3 Kbps。

配置：

[如何知道我是否限制过多的SYN数据包？](#)

如果认识您的在您的服务器的通常连接速度，您能比较图，在您启用CAR前后。比较帮助您识别一下降的出现在您的连接速度的。如果查找在速率的一下降，请增加您的CAR参数允许更多会话。

证实用户是否能容易地建立TCP会话。如果您的CAR限额太限制式，用户需要做多尝试建立TCP会话。

[能否在千兆交换路由器 \(GSR\) 上启用 CAR？](#)

可以。引擎0和引擎1线卡支持CAR。Cisco IOS软件版本11.2(14)gs2和以后提供CAR支持。CAR性能影响取决于CAR编号规定您应用。

性能影响也是极大在引擎1线卡比在引擎0线卡。如果要启用在引擎0线卡的CAR，您一定知道Cisco Bug ID [CSCdp80432 \(仅限注册用户\)](#)。如果要启用CAR到速率限制组播数据流，请保证Cisco Bug ID [CSCdp32913 \(仅限注册用户\)](#)不影响您。Cisco Bug ID [CSCdm56071 \(仅限注册用户\)](#)是您一定知道的另一bug，在您启用CAR前。

[能否在 Cisco 7500 上启用分布式 CAR \(dCAR\)？](#)

是、RSP/VIP平台支持dCAR在Cisco IOS软件版本11.1(20)CC和全部12.0软件版本。

CAR在某种程度上影响性能。凭CAR配置，您能达到线路与一VIP2-50 [through dCAR]的速率[for Internet Mix traffic]在OC3。保证Cisco Bug ID [CSCdm56071](#) (仅限注册用户)不影响您。如果要使用输出控制访问率，Cisco Bug ID [CSCdp52926](#) (仅限注册用户)能影响您的连接。如果启用dCAR，Cisco Bug ID [CSCdp58615](#) (仅限注册用户)能引起VIP崩溃。

[能否在 Cisco 7200 上启用 CAR？](#)

可以。NPE支持在Cisco IOS软件版本11.1(20)CC的CAR和全部12.0软件版本。

CAR根据CAR配置在某种程度上影响性能。获得这些Bug的修正：Cisco Bug ID [CSCdm85458](#) (仅限注册用户)和Cisco Bug ID [CSCdm56071](#) (仅限注册用户)。

注意：在接口/子接口的很大数量的CAR条目降低性能，因为路由器需要执行在CAR语句的线性搜索查找匹配的“CAR”语句。

[其他特性和选择](#)

[IP 接收 ACL](#)

Cisco IOS软件版本12.0(22)S包含在Cisco 12000SERIES互联网路由器的IP接收ACL功能。

IP接收ACL功能为被注定的流量提供基本过滤器到达路由器。因为功能过滤在入口接口的所有输入访问控制表(ACL)路由器能保护从攻击的高优先级路由协议流量。在分布式线卡的IP接收ACL功能过滤流量在路由处理器前收到数据包。此功能允许用户过滤拒绝服务充斥路由器。所以，此功能防止路由处理器的性能下降。

参考的[IP接收APL](#)欲了解更详细的信息。

[IP 源跟踪器](#)

Cisco IOS软件版本12.0(21)S支持在Cisco 12000SERIES互联网路由器的IP Source Tracker功能。Cisco IOS软件版本12.0(22)S支持在Cisco 7500系列路由器的此功能。

IP Source Tracker功能给您对关于该的流量的收集信息对您怀疑受到攻击的主机的流。此功能也允许您容易地跟踪攻击回到在网络的进入点。当您通过此功能时识别网络入口点，您能使用ACL或CAR有效拦截攻击。

参考的[IP Source Tracker](#)欲知更多信息。

[相关信息](#)

- [如何保护网络以免受 NIMDA 病毒](#)
- [IP接收APL](#)
- [IP 源跟踪器](#)
- [技术支持和文档 - Cisco Systems](#)