在12000系列Internet路由器上实施访问列表

目录

简介

本文档介绍对Cisco 12000系列互联网路由器的访问控制列表(ACL)的支持。

先决条件

要求

思科建议您了解ACL在思科路由器上的基本工作原理。

有关ACL及其应用的一般信息，请参阅以下文档：

- 访问控制列表:概述和指南

- 配置IP服务：过滤IP数据包

使用的组件

本文档中的信息基于Cisco 12000系列Internet路由器。

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。

Cisco 12000 系列互联网路由器的 ACL 支持的概述

在Cisco 12000系列互联网路由器上，ACL可以在硬件（专用集成电路 — ASIC）、软件（线卡的CPU）中处理，也可以作为混合功能在软件中处理，并辅以硬件支持。ACL是在硬件中处理还是在软件中处理取决于ACL应用、线卡引擎类型以及来自其他线卡中ACL的交互。

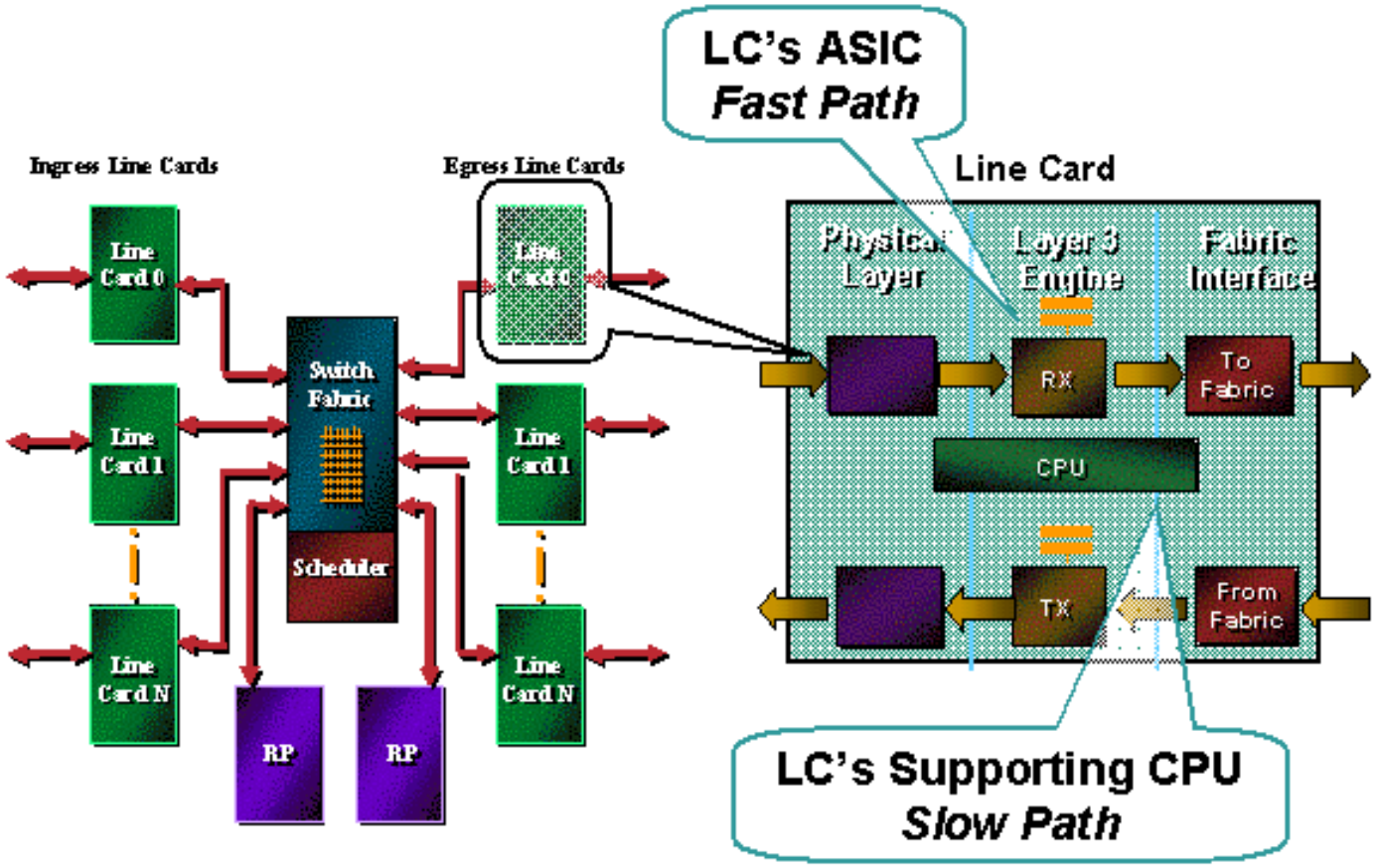
Cisco 12000系列线卡引擎提供不同的ACL功能。有关特定线卡引擎的ACL支持信息，请转至本文档中的相应部分。

注意：Cisco IOS®软件版本12.0S不支持IP组播ACL。IP组播边界功能可在需要组播过滤时使用。有关详细信息，请参阅Cisco 12000系列引擎2和ISE线卡上的快速路径组播转发。

基于 ASIC 的ACL 与基于 CPU 的 ACL 的比较

Cisco 12000支持所有代的ACL处理。要在Cisco 12000上有效地使用ACL，必须对每种处理模式的工作方式、交互方式和相互支持方式进行操作性的了解。

早期的ACL处理使用可编程CPU来处理ACL。随着时间的推移，每秒数据包数(PPS)处理要求超过了新CPU的跟上能力。ASIC旨在实现更高的PPS速率，以实现路由器转发和功能。然后，在线卡(LC)CPU上加载的ACL被加载到LC ASIC上。ASIC继续是临时的，以处理更高的PPS速率。这些第二代ASIC建立在前一代的开创性工作之上，并提供更多ASIC功能。由于Cisco 12000是分布式路由平台，因此各代ACL处理之间的交互可能会造成一些操作混乱。



本文档中使用基于ASIC的ACL、基于CPU的ACL、快速路径、慢速路径和ASIC Punts等术语，以帮助解释ACL处理的过程。以下是这些术语的解释：

- 基于ASIC的ACL（快速路径）— ACL在ASIC硬件中加载和处理。ASIC的性能包络决定了ACL的深度、性能和功能。该路径中使用了快速路径，以说明基于ASIC的处理与在支持LC的CPU中完成的处理之间的区别。本文档中使用了更通用的术语，即基于ASIC。
- 基于CPU的ACL（慢速路径）— ACL在线卡CPU上的软件中处理。对于早期的卡（引擎0，在某些情况下为引擎1），所有处理都在LC CPU上完成。基于ASIC的LC对从ASIC传送的数据包执行ACL处理。Slow Path过去用于说明到LC CPU的流量比ASIC的流量慢。本文档中使用了更通用的术语，即基于CPU。
- ASIC Punts - ASIC具有严格的设计信封。当数据包超过设计的信封时，会从ASIC发送数据包，以在支持CPU的LC上进行处理或发送到路由处理器(RP)。基于ASIC的ACL会传送不属于ASIC设计的数据包。例如，ACL的ACE带有log或log-input关键字。记录数据包所需的信息需要在ASIC外部进行处理，因此数据包会自动从ASIC传出到LC CPU中，并像基于CPU的普通ACL那样处理。

注意：当使用match语句配置基于策略的路由(PBR)以匹配ACL时，ACL不应与源端口匹配。千兆位交换机路由器(GSR)不支持PBR的硬件交换，ACL与源端口匹配。它触发进程交换，GSR性能降低。

控制和管理平面过滤

路由器处理器在Cisco 12000系列的分布式架构中提供控制和管理平面服务。接收路径ACL(rACL)为控制和管理发往RP的流量提供简单的分布式过滤功能。从逻辑上讲，它可被视为利用分布式架构优势的额外安全层。

配置 IP 接收路径 ACL

rACL通过特殊豁免引入Cisco IOS®软件版本12.0(21)S2的维护限制。Cisco IOS软件版本12.0(22)S正式支持rACL。有关详细信息，请参阅IP Receive ACL。

路由器处理器在Cisco 12000系列的分布式架构中提供控制平面服务。接收ACL提供过滤功能，用于控制发往RP的流量，例如路由更新和简单网络管理协议(SNMP)查询。

rACL被视为多阶段工作的第1阶段，旨在为平面流量的控制和管理添加新的保护。通过软件更新，新的速率限制增强功能正在添加。

线路卡类型提供的 IPv4 ACL 支持

12000系列线卡为每种引擎类型提供不同的ACL功能。本节介绍不同线卡引擎的ACL功能。有关特定线卡引擎的ACL支持信息，请参阅本文档的相应部分。

所有ACL（基于ASIC和CPU）都有一些一般特征：

- 每个方向的接口只能应用一个ACL。例如，接口POS 0/0只能有一个输入ACL和一个输出ACL。
- 根据ACL测试数据包在找到匹配项后停止。如果一个300个条目的ACL与访问列表条目(ACE)#45上的数据包匹配，则会处理该数据包并停止ACL处理。
- 每个ACL的末**尾都**有一个隐式deny all条目。因此，如果ACL上没有匹配项，数据包将被丢弃。Cisco ACL是使用显式*permit ACL架*构创建的。这意味着必须有一个ACE来匹配数据包，以便其被处理和转发。
- 新添加的ACE始终附加到ACL的末尾。每当ACL需要更新时，最好删除ACL(使用**no access-list**命令)并重新添加新ACL。
- 由于非初始IP分段在IP报头中不包含第4层协议信息，因此非初始分段仅支持标准匹配条件。有关Cisco ACL如何符合IP分段过滤的详细信息，请参阅访问控制列表和IP分段。
- 编号ACL一旦通过命令行界面(CLI)输入，就会立即进行处理并应用。 对于大型ACL，这有时会导致RP或LC CPU上出现CPU峰值。

引擎 0 - ACL 处理

引擎0是为Cisco 12000提供的第一个线卡。它全部基于CPU的处理和转发。因此，引擎0线卡在LC CPU中处理ACL。

这些线卡基于引擎0:

线卡类型	接口类型	连接性
12个DS3	同轴	SMB
12个DS3	同轴	SMB
12 x E3	同轴	SMB
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS	IR
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	LR
4xOC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	IR

1xOC12c/STM4c	POS	MM
6xCT3->DS1		SMB
2xCHOC3/STM1->DS1/E1		IR
4xOC3c/STM1c	ATM	IR
4xOC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

支持的匹配条件

引擎0支持所有Cisco IOS软件版本12.0S标准、扩展ACL和Turbo ACL。

支持的ACE数量

ACL大小仅受性能要求和可用内存资源的限制。

输出ACL处理

输出ACL在系统中其他线卡的入口功能路径中处理。将输出ACL推送到其他LC的入口端可防止背板转发即将丢弃的数据包。这是Cisco 7500上分布式架构的继承功能。IPv4输出ACL — 线卡互操作矩阵中提供了详细的说明、原因和操作指南。

线卡特定命令

无.

运营指南和线卡交互

- 如果NetFlow在引擎0线卡上配置，而输出ACL在出口引擎3或4+线卡上配置，则输出ACL由入口线卡和出口线卡处理，以便NetFlow能够处理ACL拒绝的数据包和转发的数据包。

建议

思科建议在引擎0上对大型ACL使用Turbo ACL。小型线性ACL对于小型ACL更有效，因为Turbo ACL需要额外的内存。

引擎 1 - ACL 处理

概述

引擎1线卡是引擎0上基于CPU的处理与引擎2上第一代转发/功能ASIC之间的桥接。默认情况下，引擎1线卡在软件中处理ACL。使用Cisco IOS软件版本12.0(10)S及更高版本，引擎1为配备Salsa ASIC版本4或5的卡提供硬件ACL（请参阅下面的板卡命令参考，以确定特定卡所配备的Salsa版本）。

这些线卡基于引擎1:

线卡类型	接口类型	连接性
8xFE	(RJ45)	100BaseT
8xFE	（毫米）	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	（毫米）	100BaseF
1个GE	SX、	GBIC:
1个GE	SX、	GBIC:
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	MM
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	MM

支持的匹配条件

LC CPU（慢速路径）支持所有Cisco IOS软件版本12.0S支持的标准、扩展和Turbo ACL。 此外，引擎1可以处理Salsa ASIC中的输入ACL。Salsa ASIC处理输入ACL处理和路由查找，与传统线性ACL处理和Turbo ACL处理相比，可提高性能。Salsa ASIC无法处理输出ACL或子接口ACL。

支持的ACE数量

ACL大小仅受性能要求和可用内存资源的限制。

输出ACL处理

输出ACL在系统中其他线卡的入口功能路径中处理。有关详细信息，请参阅“IPv4输出ACL — 线卡互操作矩阵”部分。

线卡特定命令

- **access-list hardware salsa**
- **show controller l3 |包括ASIC**

运营指南和线卡交互

- Salsa ASIC和PSA ASIC不能同时操作。access-**list hardware命令**仅接受PSA（引擎2）或Salsa（引擎1），但不接受两者。
- 如果NetFlow在引擎1线卡上配置，而输出ACL在出口引擎3或4+线卡上配置，则输出ACL由入口线卡和出口线卡处理，以便NetFlow能够处理ACL拒绝的数据包和转发的数据包。

建议

对于不支持硬件ACL的引擎1线卡版本，思科建议对大型ACL使用Turbo ACL。小型ACL（少于20行）可作为线性ACL实施，以节省内存。

引擎 2 - ACL 处理

概述

引擎2是第一个具有转发/功能ASIC的线卡。借助Cisco IOS软件版本12.0(10)S及更高版本，引擎2线卡在高性能分组交换ASIC(PSA)中提供硬件ACL功能。 与所有转发/功能ASIC一样，严格的性能信封也会限制ASIC的功能。引擎2 ACL上的关键性能信封是由于PSA ASIC中的内存限制。

引擎2中的数据包转发由PSA ASIC完成。PSA有三个主要的外部记忆：

- PLU（路径查找） — 用于存储mtrie节点
- TLU（表查找） — 用于存储FIB枝叶和可能的负载平衡结构。还用于容纳许多PSA ACL数据结构
- SRAM — 负载共享结构的主位置

PSA ACL功能是基于微码的ACL检查实施。PSA芯片中加载了一组特殊指令，允许进行基本ACL检查。此功能有许多限制，在部署之前应仔细了解。PSA ACL的一个主要缺点是需要大量硬件转发内存。

PSA ACL功能需要预分配大块PLU/TLU内存，而不管前缀的数量如何等。由于此分配主要来自TLU区域，因此在配置PSA ACL时，它会对这些卡上可维护的路由数量产生重大影响。

除了PLU/TLU内存的初始开销外，存储在TLU内存中的每个前缀都需要显着增加的内存。每个前缀所需的内存量会因所应用ACL的方向（入口与出口）和线卡类型而异。一般而言，出口ACL比入口ACL需要更多的内存，而物理端口较多的线卡需要的内存比端口较少的线卡需要的内存更多。

如果引擎2线路卡不使用ACL，则无论实际配置的ACL如何，都会构建ACL的数据结构。要更改为较小的非ACL结构，必须在路由器**上配置no access-list** hardware psa。此命令禁用所有Engine2线卡上所有方向的所有ACL处理。思科建议谨慎使用。

概述

为了提供与匹配深度无关的ACL处理性能，引擎2 ACL集成到硬件转发表中。有关这会如何影响前缀可扩展性的说明，请参阅下文。

这些线卡基于引擎2:

线卡类型	接口类型	连接性
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM6	启用程序	SR

4c		
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	ATM	IR
4xOC12c/STM4c	ATM	MM
8xOC3cSTM1c	ATM/TS	IR
8xOC3c/STM1c	ATM/TS	MM
3xGE	SX	GBIC:
3xGE	CWDM	GBIC:
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR

支持的匹配条件

除第4层源端口外，所有Cisco IOS软件版本12.0S支持的标准ACL和扩展ACL匹配条件。不连续掩码、IP优先级字段和第4层源端口从PSA ASIC传送，并在LC CPU上处理。

支持的ACE数量

在PSA中最多五个448行输入ACL。每个端口可配置一个ACL。其他ACL由线卡CPU管理。有关输出ACL的限制，请参阅下面的“限制”部分。

输出ACL处理

在此线卡上配置的输出ACL将在系统中其他线卡的入口功能路径中执行。有关详细信息，请参阅IPv4输出ACL — 线卡互操作矩阵。

线卡特定命令

- access-list hardware psa limit 128
- no access-list hardware psa
- PSA旁路
- show access-list psa detail
- show access-list psa summary
- show controller psa feature

运营指南和线卡交互

- 快速路径ACL处理需要满足以下条件：应用的ACL在128或448 ACE限制内。如果配置了access-list hardware psa limit 128命令，**则长度必须小于128**个ACE。当需要448行ACL微码捆绑时，长度必须小于448个ACE。输入和输出ACL并非按卡一起配置。路由器上最多可配置五个输出*ACL*。
- 8和16端口OC-3/STM-1 POS线卡仅支持128行ACL。4端口OC-12/STM-4 POS、1端口OC-48/STM-16 POS和3端口千兆以太网线卡支持448个线路ACL。
- 当两个ACL同时配置在同一卡上时，在快速路径中，输入ACL优先于输出ACL（输出ACL在慢速路径中处理）。
- 如果在引擎2卡上配置了输出ACL，而入口线卡是引擎0/1/2/4，则输出ACL将在入口卡中处理。对于其他引擎类型，输出ACL将在引擎2出口慢速路径中处理。
- IP到MPLS流量不支持输出ACL（第一个MPLS标签被“推送”到IP数据包）。
- ACL处理信息已集成到硬件FIB中，并可能影响前缀的可扩展性。前缀内存耗尽由内存分配失败报告，并在随附的日志消息中使用“exmem=1”签名。

建议

- ACL处理信息会集成到CEF转发表中，这会降低前缀的可扩展性。不使用ACL的应用可以在CEF表中禁用ACL支持，从而通过发出no access-list hardware psa命令**增加可用前缀**内存。
- 配置no access-list hardware psa**命令可禁用引擎2卡的所有ACL处理，并禁用对ACL的PSA支持。**它不强制软件执行ACL。如果出口线卡配置了输出ACL，则此情况也适用。
- 在access-list hardware psa命**令后对access-list compiled**命令的配**置，可将超过PSA容量的ACE转换为Turbo ACL。**这为长度超过448个ACE的ACL提供最佳ACL性能。默认ACL微码为128(与Cisco IOS软件版本12.0(14)S/ST相同)。 如果使用的ACL较小，并且不需要448线路功能，则配置**access-list hardware psa limit 128** 命令可节省转发(TLU)内存，这可提高前缀可扩展性。对于长度超过129行的ACL，应使**用access-list compiled命令**以及access-list hardware psa limit 128命**令启用Turbo ACL处理**功能。此组合使用Turbo ACL处理PSA ASIC中的前128条线路和其余线路，这样可优化性能，同时节省转发内存。
- 4端口OC12 ATM线卡不支持输入ACL，但提供微码输出ACL检测，允许在慢速路径中输出ACL。
- 8xOC3 ATM线卡支持每条VC 128线路ACL，采用Cisco IOS软件版本12.0(23)S及更高版本。在快速路径中最多可配置16个不同的输入ACL。448输入ACL仅在慢速路径中以每条VC为基础。不支持输出ACL。

ISE（IP 服务引擎）引擎 3 - ACL 处理

概述

引擎3是第一个双级转发线卡。引擎3在入口和出口路径上具有转发/功能ASIC。这允许ACL在入口和出口路径上放置在ASIC中。此外，引擎3 ASIC结构是混合管道/并行阵列。ASIC结构在并行高速三态内容可寻址存储器(TCAM)中实施ACL处理，该存储器为每个入口提供高达20K ACE和每个出口20K ACE的线速处理。

这些线卡基于引擎3:

线卡类型	接口类型	连接性
4xOC12c/STM4c	POS	IR

4xOC12c/STM4c	POS	MM
4xCHOC12/STM4->OC3/STM1->DS3/E3	POS	IR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
8xOC3/STM1c	POS	IR
8xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	IR
4xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xCHOC48/STM16->STM4->OC3/STM1->DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	IR
4xOC12c/STM4c	ATM/IP	MM
4xGE	GE	
4xOC12c/STM4c	DPT	IR
4xOC12c/STM4c	DPT	XLR

支持的匹配条件

除线卡CPU处理的日志ACE外，快速路径支持所有Cisco IOS软件版本12.0S标准和扩展匹配条件。

支持的ACE数量

- 每个端口、每个VLAN、每个帧中继子接口和每个ATM子接口在入口和出口方向进行线速处理。每个方向和每个卡支持多达20,000个扩展ACE。
- TCP/UDP源/目标端口“range”、“lt”和“gt”的匹配条件均在硬件中使用“L4操作员”资源处理。
- 整个线卡的不同L4操作数数限制为32。源端口操作符最多限制为6个。

输出ACL处理

在传输路径数据包处理ASIC中为线速输出ACL处理提供本地快速路径支持。有关详细信息，请参阅IPv4输出ACL — 线卡互操作矩阵。

线卡特定命令

- **hw-module <*slot #*> tcam compile no-merge*!—12.0(21)S3***
- **show-access-list hardware interface <*interface name*>**
- **show cef int pos[*x/y*] | inc if_number**

运营指南和线卡交互

- 匹配日志记录ACE的数据包在慢速路径中处理。
- 匹配deny ACE的数据包（为防止系统中断而限制）在慢速路径中处理。
- 当ACL包含一系列地址时，硬件使用称为“范围ACE”的特殊ACE，这些ACE最多需要三个ACE。
- ACL合并可通过在各个ACL之间共享通用ACE来节省TCAM资源。要确定是否合并了ACL，请使用**show-access-list hardware interface命**令。
- 合并的ACL不支持ACL计数器。对于Cisco IOS软件版本12.0(21)S3及更高版本，可以使用**hw-module <slot #> tcam compile no-merge命令禁用ACL合**并。要确定是否合并了ACL，请使用**show-access-list hardware interface命**令。
- 如果NetFlow在引擎0/1线卡上配置，而输出ACL在出口引擎3或4+线卡上配置，则输出ACL将由入口和出口线卡处理，以便NetFlow能够处理ACL拒绝的数据包和转发的数据包。

ACL计数器支持

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

定义：

- Per-ACE — 正常的Cisco IOS软件支持，RP/LC上的**show access-list <*number*>**命令显示与每个ACE关联的ACL和计数器。只有在配置任何ACL之**前禁**用合并时，它才可用。这可以通过以下配置命令来完成：

  ```
  Router(config)#hw-module slot <number> tcam compile acl no-merge
  ```

  启用此选项后，会关闭某些TCAM合并优化并影响可扩展性。具体效果取决于单个ACL。另请注意，如果在该接口上应用基于策略的路由，则计数器将不正确。在这种情况下，应使用聚合计数器。
- Per-ACE(TCAM) — 与每个TCAM条目关联的硬件计数器。无需配置，对性能/可扩展性没有影响。仅使用此CLI在线卡上可用。软件无法清除这些计数器。

  ```
  LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace
  ```

  Cisco IOS软件版本22S中将提供此命令的新通用CLI:

  ```
  LC-Slot4#show access-list hardware interface p0:1 in
  ```

  与per-ACE计数器一样，TCAM计数器仅在ACL接口上未使用PBR时有效。
- 聚合 — 每个ACL显示一个摘要允许/拒绝计数器。这是所有单个ACE计数器的总和。无需配置，对性能或可扩展性没有影响。

建议

目前没有。

引擎 4 (POS) - ACL 处理

概述

引擎4通过Cisco IOS软件版本12.0(18)S及更高版本提供此ACL支持：

- 如果引擎4线卡是入口卡，则E0/1/2线卡支持输出ACL。在此配置中，输出ACL由出口线卡CPU处理。

这些线卡基于引擎4:

线卡类型	接口类型	引擎类型	连接性
4xOC48c/STM16c	POS	E4	
4xOC48c/STM16c	POS	E4	LR
1xOC192c/STM64c	POS	E4	IR
1xOC192c/STM64c	POS	E4	SR
1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

引擎 4+（POS 和 DPT）- ACL 处理

概述

引擎4+为Cisco 12000系列万兆产品组合引入了ACL功能。

每个入口和出口路径最多支持1024个ACE。输入和输出ACL都以线速处理，最多96个ACE。长匹配的性能因匹配深度而异。

这些POS线卡基于引擎4+:

线卡类型	接口类型	连接性
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LR
1xOC192c/STM64c	POS	IR
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LR
4xOC48c/STM16c	DPT	SFP:

1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

支持的匹配条件

除日志或分段ACE外，快速路径支持所有Cisco IOS软件版本12.0S支持的标准和扩展ACL条件。

支持的ACE数量

在快速路径中，每个方向最多支持1024个ACE。

注意：ACE的1021是可配置的。为ACE隐式permit ip any any、**deny ip any any** 和**send to CPU命令保留三个条**目。

支持的ACE数量没有上限。超过1021限制的任何ACE都在线卡慢速路径中执行。

输出ACL处理

输出ACL在传输端快速路径中处理。有关详细信息，请参阅IPv4输出ACL — 线卡互操作矩阵。

线卡特定命令

- **show tcam appl [*acl-in* | *acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in* | *acl-out*]内存<*port*> <*条目数*>**

运营指南和线卡交互

- 不支持子接口ACL。
- 性能随匹配深度而变化。
- 范围条目使用两个ACL规则（如果两个条目跨越边界则使用三个）。
- 每个物理接口支持一个ACL。
- 快速路径最多支持1024个ACE（每个方向）。
- 1024个快速路径ACE中的任何一个都可以在端口之间共享。
- 使用fragment关键字的ACE在慢速路径中过滤。
- 在慢速路径中处理的ACE不计入被拒绝的数据包。
- 如果NetFlow在引擎0线卡上配置，而输出ACL在出口引擎3或4+线卡上配置，则输出ACL将由入口和出口线卡处理，以便NetFlow能够处理ACL拒绝的数据包和转发的数据包。

建议

目前没有。

引擎 4+（以太网）- ACL 处理

概述

引擎4+以太网线卡在硬件中引入了每VLAN输入ACL功能，用于Cisco 12000万兆以太网产品组合。以下是一些特征：

- 输入和输出ACL可同时应用于单个端口，而不会影响性能。
- ACL可以按VLAN或按端口应用。
- 输入ACL性能高达15K ACE，但匹配深度不会降低。
- 输出ACL以线速处理，最多96个ACE。长匹配的性能因匹配深度而异。

以太网线卡基于引擎4+:

线卡类型	接口类型	引擎类型
10xGE修订版B(“X-B”)	SFP:	E4+
模块化	SFP:	E4+
1个10GE	10G	E4+
1个10GE	10G	E4+

支持的匹配条件

除日志或分段ACE外，快速路径支持所有Cisco IOS软件版本12.0S支持的标准和扩展ACL条件。

支持的ACE数量

- 最多15,000个输入ACL，可以按端口或按VLAN配置。
- 每个卡1024个输出ACE，可按端口应用。**注意：**ACE的1021是可配置的。为ACE隐式permit ip any any、**deny ip any any** 和**send to CPU命令保留三个条**目。

输出ACL处理

输出ACL在传输端快速路径中本地处理。有关详细信息，请参阅IPv4输出ACL — 线卡互操作矩阵。

线卡特定命令

- **hw-module slot <*number*> ip acl merge**

运营指南和线卡交互

- 包含fragment关键字的ACE在慢速路径中处理。
- ACL与其他功能结合使用时不支持ACL计数器。
- 合并的ACL不支持ACL计数器。合并的ACL可通过**hw-module slot <slot number> ip acl merge命令进行配置**。
- 每个线卡支持多达168个L4操作。超过此值后，ACL将在慢速路径中运行。
- 如果引擎1线卡已启用采样NetFlow，并且出口引擎3或4+线卡上启用了输出ACL，则入口和出

口线卡都会处理输出ACL，以便NetFlow能够处理ACL拒绝的数据包和转发的数据包。

建议

目前没有。

ACL 记录

在Cisco IOS软件版本12.0(21)S之前，ACL日志记录信息仅通过维护总线(MBUS)发送到RP。 在ACL日志记录活动的高级别期间，可能会超出MBUS的容量。思科IOS软件版本12.0(21)S引入了几种防止此场景的优化。

Cisco IOS软件报告MBUS过载情况，并显示以下错误消息：

```
LCLOG-3-INVSTATE

MBUS_SYS-3-SEQUENCE
```

使用Cisco IOS软件版本12.0(21)S及更高版本，高严重性（严重性0-4）日志记录消息通过MBUS传送到RP，而低严重性（严重性5-7）日志消息通过高容量交换矩阵传送到RP。ACL日志消息严重性较高，因此现在通过交换矩阵传送到RP。

此添加的日志记录功能可使用以下命令进行配置：

- logging method mbus [*severity*] — *按严重性确定哪些消息将使用MBUS发送到RP。*更高严重性的消息将通过交换矩阵发送。
- **show logging method** — 显示所有消息严重性级别的当前日志记录方法。
- **logging sequence-nums** — 此命令使发送线路卡能够对序列号日志消息进行排序，以便RP能够正确地对消息重新排序。如果没有此命令，日志消息可以按非顺序顺序传送到RP。

IPv4 输出 ACL - 线路卡互操作矩阵

在引入Engine 3和Engine 4+版本的出口ACL处理之前，输出ACL由入口线卡处理。输出ACL已更新，以利用高性能引擎3和引擎4+输出ACL处理功能。

此图表汇总了不同线卡组合的输出ACL的处理位置：

	出口线卡					
入口线卡（应用于成员接口的输出ACL）	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	入口	入口	入口	出口	不适用	出口
E1	入口	入口	入口	出口	不适用	出口
E2	入口	入口	入口	出口	不适用	出口
E3	出口	出口	出口	出口	不适	出口

					用	
E4	出口	出口	出口	出口	不适用	出口
E4+	出口	出口	出口	出口	不适用	出口

IPv6 ACL 支持

Cisco IOS软件版本12.0(23)S中E0、E1、E2、E3和E4+的慢速路径（入口和出口）支持IPv6扩展ACL。

在引擎3中，Cisco IOS软件版本12.0(25)S的硬件支持IPv6 ACL功能。ACL应用于特定接口，每个访问列表末尾都有一条隐式deny语句。IPv6 ACL在全局配置模式下使用**ipv6 access-list**命令和deny和permit关键字进行配置。基于引擎3的卡支持过滤基于流量的IPv6选项报头、流标签和（可选）上层协议类型信息。

Cisco 12000 ACL 命令参考

引擎1命令

- access-list hardware salsa
- show controller l3 |包括ASIC

引擎2命令

- access-list hardware psa limit 128
- no access-list hardware psa
- PSA旁路
- show access-list psa detail
- show access-list psa summary
- show controller psa feature

引擎3命令

- hw-module <*slot #*> tcam compile no-merge*! — 自Cisco IOS软件版本12.0(21)S3起*
- show-access-list hardware interface <*interface name*>
- show contr [*tofab|frfab*] alpha acl <*int*> vmr2ace

引擎4+命令

- show access-list gen7 label
- show tcam appl [*acl-in | acl-out*] tcam <*label-no*>
- show tcam appl [*acl-in | acl-out*]内存<*port*><*条目数*>

引擎4+以太网命令

- hw-module slot <*number*> ip acl merge

词汇表

本节提供相关术语的标准定义：

- **处理平面** — 网络设备可以逻辑地划分为三个处理平面：数据平面 — 对流经网络设备的数据包进行处理。控制平面 — 对用于将网络设备粘合在一起的数据包进行处理。这包括线路协议（如点对点协议 — PPP和高级数据链路控制 — HDLC）、路由协议（边界网关协议 — BGP、路由信息协议第2版 — RIPv2、开放最短路径优先 — OSPF等）和计时协议（如网络时间协议） — NTP)。管理平面 — 对用于管理网络设备的数据包进行处理。这包括telnet、安全外壳(SSH)、文件传输协议(FTP)、简单文件传输协议(TFTP)、SNMP和其他管理协议。
- **标准ACL** — 标准ACL仅在第3层过滤。
- **扩展ACL** — 扩展IP访问列表使用源地址和目标地址进行匹配操作，并使用可选协议类型信息进行更精细的控制。
- **线性处理的ACL** — 在软件中线性处理。性能随匹配深度而变化（在确定匹配之前必须检查的条目数）。
- **Turbo ACL（已编译）** - Turbo ACL通过将ACL编译为一系列高度优化的查找表来优化软件ACL处理，从而加快软件处理速度。Turbo ACL的性能不随匹配深度而变化。
- **输入ACL** — 应用于进入应用该ACL的端口的流量的ACL。
- **输出ACL** — 应用于从应用该ACL的端口发出的流量的ACL。除了一些例外，输出ACL由输入线卡处理。
- **Receive Path ACLs** - Receive Path ACLs提供对发往路由器本身的控制流量（例如路由更新和SNMP查询）的过滤。
- **双级转发线卡** — 在入口和出口路径上具有转发/功能ASIC的线卡。这允许线卡在入口数据包流和出口数据包流上同时执行功能，而不将数据包发送到LC CPU。它还允许在Cisco 12000中使用新的双级转发算法。引擎3线卡是双级转发线卡的示例。
- **单级转发线卡** — 在入口路径上具有转发/功能ASIC的线卡。这些线卡仅对在入口路径上流动的数据包执行基于ASIC的处理。出口流量不会处理（仅转发）、由其他LC的入口ASIC处理或由LC CPU管理。引擎2、引擎4和引擎4+是单级转发线卡的示例。

相关信息

- Cisco 12000 系列互联网路由器
- 技术支持和文档 - Cisco Systems