GSR:接收访问控制列表

目录

简介

本文描述称为接收访问控制列表(rACLs) 1的新安全功能，并提供了rACL配置的建议和指南。通过防止路由器的千兆路由处理器(GRP)处理多余和潜在恶毒数据流，接收ACL能够用于增强Cisco 12000路由器安全。接收 ACL 作为一个特殊的放弃被添加到 Cisco IOS® 软件版本 12.0.21S2 的维护扼杀中，并集成到了 Cisco IOS 软件版本 12.0(22)S 中。

GRP 保护

千兆交换路由器(GSR)接收的数据可以分开成两个大类别：

- 经由转发路径通过路由器的数据流。
- 必须经由接收路径发送到 GRP 以供进一步分析的数据流。

在正常运行中，大部分数据流只是经过GSR en route，流向其它目的地。然而，GRP必须处理特定类型的数据，主要是路由协议、远程路由器访问和网络管理数据流(例如简单网络管理协议[SNMP])。 除上述数据流以外，其他第 3 层数据包也可能需要 GRP 的处理灵活性。这将包括某些 IP 选项和某些形式的 Internet 控制消息协议 (ICMP) 数据包。参见接收邻接信息包和丢弃信息包的附录，了解有关rACL和GSR 接收路径数据流的详细信息。

GSR 有多个数据路径，每个路径分别处理不同形式的数据流。转接流量从进入线路卡(LC)先转发到光纤，然后转发到输出卡上，为下一跳交付做准备。除转接流量数据路径外，GSR还提供要求本地处理数据流的另外二条路径：LC 到 LC CPU 以及 LC 到 LC CPU 到结构再到 GRP。下表列出了几个常用功能和协议的路径。

流量类型	数据路径

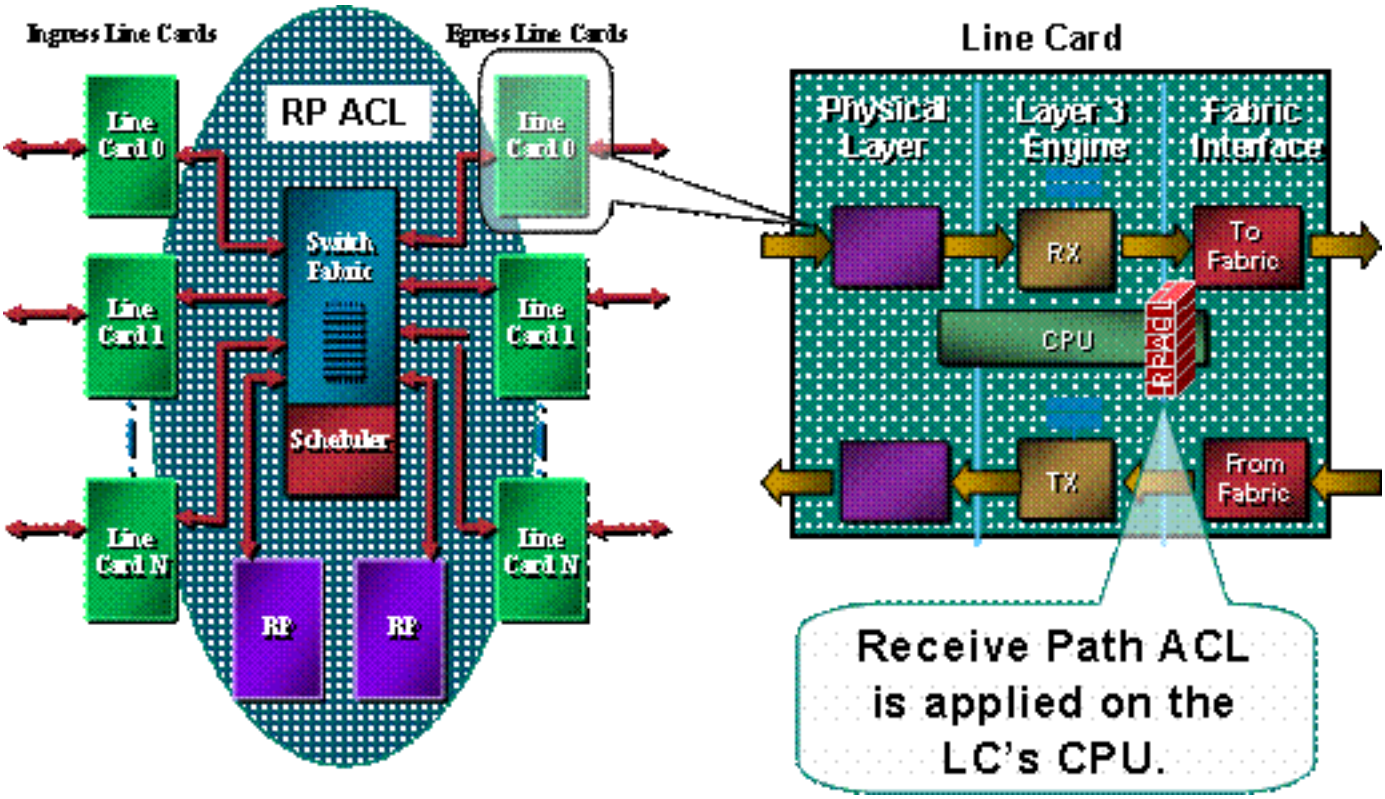
正常（中转）数据流	LC 到结构再到 LC
路由协议/SSH/SNMP	LC 到 LC CPU 到结构再到 GRP
ICMP Echo (ping)	LC 到 LC CPU
日志记录	

在处理从 LC 发往 GRP 本身的数据流时，GSR 路由处理器的容量比较有限。如果大量数据需要传送到 GRP，该数据流可能会使 GRP 过载。这将造成一次有效的拒绝服务 (DoS) 攻击。GRP 的 CPU 力求跟上数据包检查速度，并且开始丢弃数据包，使输入保留和选择性数据包丢弃 (SPD) 队列泛洪。[2] GSR应针对三种情况进行保护，这三种情况可能是针对路由器GRP的DoS攻击所致。

- 正常优先级泛洪导致的路由协议数据包丢失
- 正常优先级泛洪导致的管理会话（Telnet、Secure Shell [SSH]、SNMP）数据包丢失
- 伪装的高优先级泛洪导致的数据包丢失

正常优先级溢出阶段的路由协议数据所带来的潜在损失可以通过静态数据流分类和从LC上限制定向于GRP的数据流速率实现。遗憾的是，此方法存在局限性。如果进攻是通过几个LC交付的，要保护高优先级路由协议数据，仅限制目的地为GRP的正常优先级数据流速率是不够的。将丢弃正常优先级数据以提供保护的阈值降低只能加剧正常优先级泛洪导致的管理数据流损失。

如下图所示，在数据包传输到 GRP 之前，会在每个 LC 上执行 rACL。



需要对 GRP 采用一种保护机制。由于接收邻接，rACL 会影响发送到 GRP 的数据流。接收邻接是发往路由器 IP 地址的数据流所拥有的 Cisco 快速转发邻接，例如广播地址或配置在路由器接口上的地址。[3]有关接收邻接关系和已转发数据包的详细信息，请参阅附录部分。

进入 LC 的数据流首先会发送到 LC 的本地 CPU，需要由 GRP 进行处理的数据包会排队等候转发至路由处理器。接收ACL在GRP创建，并流向不同LC的CPU。数据流从 LC CPU 发送到 GRP 之前，会与 rACL 进行比较。如果允许，数据流通到GRP，而其它数据流被拒绝。在执行 LC 到 GRP 速率限制功能之前，会先检查 rACL。由于rACL用于所有接收邻接，由LC CPU处理的部分信息包(例如ECHO请求)也要进行rACL过滤。设计 rACL 条目时需要考虑这一点。

接收ACL是几部分程序机制范围的第一部分，可以保护路由器资源。将来会在 rACL 中增加速率限制组件。

性能影响

没有浪费内存，除非需要具有单个配置条目和定义的访问控制列表。将rACL复制到每个LC，因此在每个LC上使用内存区域的一小部分。总之，占用的资源极少，特别是与部署的优势相比时。

接收 ACL 不会影响转发数据流的性能。rACL 仅适用于接收邻接数据流。转发的数据流从不会受到 rACL 的影响。中转数据流通过使用接口 ACL 进行过滤。这些“常规”ACL 会在指定方向应用于接口。在rACL处理之前，流量需要经过ACL处理，因此rACL不会接收被接口ACL拒绝的流量

执行实际过滤的LC(换句话说，LC接收由rACL过滤的数据流)由于rACL处理的缘故，将增加CPU利用率。然而，此CPU利用率增加是由流向GRP的大量数据流引起的;rACL 保护对 GRP 的好处远远超过在 LC 上增加的 CPU 使用率。LC 上的 CPU 使用率会根据 LC 引擎类型而异。例如，如果发生同样的攻击，引擎3 LC的CPU利用率低于引擎0 LC。

启用涡轮ACL (通过使用access-list 编辑命令)将ACL转换 成查找表条目中非常有效的系列。当 Turbo ACL 启用时，rACL 深度不会影响性能。换言之，处理速度与 ACL 中的条目数量无关。如果 rACL很短，涡轮ACL就不会大大提高性能，而只是占用内存。rACL 较短时，编译 ACL 可能不是必需的。

，通过保护GRP，rACL能确保路由器和网络在攻击期间的稳定性。如上所述，rACL是在LC CPU上处理的，因此当大数据量定向到该路由器时，每个LC上的CPU利用率都将增加。在E0/E1和一些E2套件上，100+%的CPU利用率也许会导致路由协议和链路层丢弃。这些丢弃局限到卡中，并且保护GRP路由进程，因而维护稳定性。启用限制的微码5的E2卡在负载较重时激活限制模式，并且仅将优先级6和7流量转发到路由协议。其他引擎类型具有多队列体系结构；例如，E3卡有到CPU的三个队列，同时单独的、高优先级的队列提供路由协议信息包(优先次序6/7)。除非高优先次序信息包所致，否则高LC CPU不会导致路由协议丢弃。对于发送到优先级较低的队列中的数据包，会对其执行尾部丢弃。最后，基于E4的卡有八个对CPU的队列，其中一队专用于路由协议信息包。

语法

接收ACL与下列全局配置命令一起使用，用来将rACL分配到路由器中的每个LC上。

```
[no] ip receive access-list
```

在此语法中，**<num> 定义如下：**

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

基本模板和 ACL 示例

为了使用此命令，您需要定义访问控制列表，该列表识别允许与路由器交谈的数据流。访问控制列表需包括两个路由协议和管理数据流(边界网关协议[BGP]，开放式最短路径优先[OSPF]，SNMP，SSH，Telnet)。 有关详细信息，请参阅部署准则部分。

以下示例ACL提供了一个简单概要，并展示了可用于特定用途的配置示例。该 ACL 说明了通常所需的几种服务/协议需要进行的配置。对于 SSH、Telnet 和 SNMP，使用环回地址作为目标。对于路由协议，则使用实际接口地址。在rACL中使用路由器接口取决于本地站点策略和操作。例如，如果回环用于所有BGP对等会话中，那么只有那些回环才需要BGP许可语句的允许。

```
!--- Permit BGP. access-list 110 permit tcp host bgp_peer host loopback eq bgp !--- Permit OSPF.
access-list 110 permit ospf host ospf_neighbor host 224.0.0.5 !--- Permit designated router
multicast address, if needed. access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip !--- Permit Enhanced Interior
Gateway Routing Protocol (EIGRP). access-list 110 permit eigrp host eigrp_neighbor host
224.0.0.10 access-list 110 permit eigrp host eigrp_neighbor host local_ip !--- Permit remote
access by Telnet and SSH. access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet !--- Permit SNMP.
access-list 110 permit udp host NMS_stations host loopback eq snmp !--- Permit Network Time
Protocol (NTP). access-list 110 permit udp host ntp_server host loopback eq ntp !--- Router-
originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). access-list 110 permit icmp any any ttl-exceeded access-list
110 permit icmp any any port-unreachable !--- Permit TACACS for router authentication. access-
list 110 permit tcp host tacacs_server router_src established !--- Permit RADIUS. access-list
110 permit udp host radius_server router_src log !--- Permit FTP for IOS upgrades. access-list
110 permit tcp host image_server eq ftp host router_ip_address access-list 110 permit tcp host
image_sever eq ftp-data host router_ip_address
```

对于所有Cisco ACL 来说，在访问控制列表结尾处都有一个隐藏的Deny语句，因此任何与ACL中的条目不匹配的数据流都将被拒绝。

注意： log关键字可用于帮助对发往不允许的GRP的流量进行分类。虽然日志关键字提供了详细的ACL击中的宝贵资料，但过多地使用该关键字击中ACL条目将增加LC CPU的利用率。与日志记录相关的性能影响会因 LC 引擎类型而异。通常，只有引擎0/1/2需要时才应使用日志记录。对于引擎3/4/4+，由于CPU性能提高和多队列架构，日志记录的影响要小得多。

此访问控制列表的粒度水平取决于本地安全策略(例如OSPF邻居要求的过滤级别)。

rACL 和分段数据包

ACL 含有一个 **fragments 关键字，用于启用专门的分段数据包处理行为。**通常情况下，与 ACL 中的 L3 语句（不考虑 L4 信息）相匹配的非初始分段会受到匹配条目的 **permit 或 deny 语句影响。**请注意，使用 **fragments 关键字可以强制 ACL 更精细地拒绝或允许非初始片段。**

在 rACL 上下文中，过滤分段会添加一个额外的保护层来防御仅使用非初始分段的 DoS 攻击（例如 FO > 0）。 在 rACL 开头为非初始分段使用 **deny 语句，可拒绝所有非初始分段访问路由器。**在很少的情况下，一个有效的对话可能需要分段，并且如果rACL中存在拒绝分段语句，这时它可能被过滤掉。

例如，请考虑如下所示的部分 ACL。

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
<rest of ACL>
```

将这些条目添加到 rACL 的开头可拒绝任何非初始化分段访问 GRP，而未分段的数据包或初始分段会通过 rACL 接下来的几行，而不受 **deny fragment 语句影响。**由于每个协议--通用数据报协议

(UDP)、TCP和ICMP"--增量分割ACL上的计数，上面的rACL片断还能简化攻击的分类过程。

有关选项的详细讨论，请参阅访问控制列表和 IP 分段。

风险评估

保证rACL不过滤重要流量，例如路由协议或到路由器的交互式访问。过滤必要的数据流能导致无法远程访问路由器，因而需要控制台连接。因此，实验室配置应该尽可能密切地模仿实际部署。

和往常一样，Cisco建议在配置之前，您在实验室里测试此功能。

附录和备注

接收邻接和传送的数据包

如本文档上文所述，有些数据包需要进行 GRP 处理。这些数据包从数据转发平面传送到 GRP。下面列出了需要 GRP 访问的第 3 层数据的常见形式。

- 路由协议
- 多播控制数据流（OSPF、热备用路由器协议 [HSRP]、标记分配协议 [TDP]、独立于协议的多播 [PIM] 等）
- 需要分段的多协议标签交换 (MPLS) 数据包
- 带有某些 IP 选项（如路由器警报）的数据包
- 多播流的第一个数据包
- 需要重组的分段 ICMP 数据包
- 所有数据流指定到路由器(LC 上处理的数据流除外)。

因为rACLs适合接收邻接，rACL过滤没有踢对到GRP但属于接收邻接的部分数据流上。该情况最常见的示例是 ICMP echo 请求 (ping)。定向到路由器的 ICMP echo 请求由 LC CPU 处理；因为这些请求为接收邻接，所以也由 rACL 进行过滤。因此，要允许对路由器的接口（或回环）执行 ping 操作，rACL 必须明确允许 echo 请求。

使用 **show ip cef 命令可以查看接收邻接。**

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

部署指南

Cisco 建议您采用保守部署实践。要成功部署rACL，必须熟知现有的控制和管理平面访问需求。在一些网络中，确定创建过滤器列表所需的确切的数据流配置文件可能是困难的。以下指南描述了部署rACL的极其保守的方法，使用迭代rACL帮助识别并最终过滤流量。

1. **使用分类 ACL 标识网络中使用的协议。**部署一个 rACL，使其允许访问 GRP 的所有已知协议。这种“发现”rACL 的源地址和目标地址都应设置为 **any**。可以使用记录开发匹配协议许可语句的源地址列表。除协议permit语句之外，在rACL的结尾的permit any any log 行可以用来识别

将由rACL 过滤、并且可能要求GRP访问的其他协议。目的是确定特定网络使用哪些协议。应使用记录来进行分析，以确定“还有什么”可能与该路由器进行沟通。**注意**：尽管**log**关键字提供了对ACL命中详细信息的宝贵见解，但使用此关键字的ACL条目的过多命中可能导致大量日志条目和路由器CPU使用率较高。仅当需要时才能暂时使用 **log 关键字，以便帮助对数据流进行分类。**

2. **检查已标识的数据包，并开始过滤对 GRP 的访问。**一旦在步骤1中由rACL过滤的信息包被识别并查看过，请用permit any any 语句部署rACL，供允许的协议使用。正如步骤 1，日志关键字能够提供关于匹配许可条目的数据包的更多信息。在末端使用deny any any log有助于识别指定到GRP的任何未预设的信息包。此rACL将提供基本的保护，并且允许网络工程师确保允许全部所需的数据流。目标是在没有明确的IP源地址和目的地地址范围的情况下，测试需要与路由器进行通信的协议范围。
3. **限制源地址的一个宏观范围。**只允许您分配的无类别域内路由(CIDR)块作为源地址。例如，如果为您的网络分配了171.68.0.0/16，则只允许171.68.0.0/16中的源地址。此步骤在不中断任何服务的情况下缩小了风险范围。它还从可能访问您设备的CIDR模块外部提供设备/人数据点。所有外部地址都将丢弃。由于会话允许的源地址位于CIDR块外，外部BGP对等体需要例外。此阶段可能会保留几天，为下一阶段缩小rACL收集数据。
4. **将 rACL permit 语句的范围缩小为仅允许已知且经过授权的源地址。**将源地址逐渐限制为仅允许与 GRP 通信的源。
5. **限制rACL上的目标地址(*可选*)**一些网络服务提供商(ISP)可能选择只允许特定协议在路由器上使用特定目的地地址。这个最终阶段意味着限制将接收某个协议的数据流的目的地地址范围。[6]

部署示例

下面的示例显示接收ACL保护层基于下列编址的路由器。

- ISP 的地址块为 169.223.0.0/16。
- ISP 的基础架构块为 169.223.252.0/22。
- 路由器的环回为 169.223.253.1/32。
- 该路由器是核心骨干网路由器，因此只有内部 BGP 会话处于活动状态。

提供此信息，开始接收的ACL可能与下面的示例类似。因为我们知道基础设施地址块，所以我们将首先允许整个块。稍后将添加更加详细的访问控制条目(ACE)，因为需要路由器接入的所有设备已经获得具体地址。

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.

!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
```

```
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 - Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example - Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

备注

1. 请参阅了解选择性数据包丢弃 (SPD) 和有关增强 DoS 防御的保持队列准则。
2. 有关 Cisco 快速转发和邻接的详细信息，请参阅 Cisco 快速转发概述。
3. 如需获得ACL部署指导及相关命令的详细讨论，请参考在Cisco 12000系列互联网路由器上实施ACL的章节。
4. 这里指 Vanilla、Border Gateway Protocol Policy Accounting(BGPPA)，每接口速率控制(PIRC)和帧中继数据流策略(FRTP)套件。
5. 接收路径保护的第II阶段将允许创建管理接口，自动限制哪个IP地址将监听流入信息包。

相关信息

- 访问列表支持页面
- 技术支持 - Cisco Systems