GSR:接收存取控制清單

目錄

簡介

本檔案介紹稱為接收存取控制清單(rACL)[1]的新安全功能，並提供rACL部署的建議和准則。接收ACL是用來防止路由器的Gigabit路由處理器(GRP)接收不必要且可能存在惡意的流量，以提高Cisco 12000路由器的安全性。接收ACL是以Cisco IOS ®軟體版本12.0.21S2之維護節流的特殊免責方式新增，而且已整合到Cisco IOS軟體版本12.0(22)S中。

GRP保護

Gigabit交換器路由器(GSR)接收的資料可分為兩大類：

- 通過轉發路徑通過路由器的流量。
- 必須通過接收路徑傳送到GRP以進行進一步分析的流量。

在正常操作中，大部分流量只是通過GSR到達其他目的地。但是，GRP必須處理特定型別的資料，最明顯的是路由協定、遠端路由器訪問和網路管理流量（如簡單網路管理協定[SNMP]）。 除了此流量，其他第3層資料包可能需要GRP的處理靈活性。其中包括某些IP選項和某些形式的網際網路控制訊息通訊協定(ICMP)封包。請參閱接收鄰接和傳輸資料包的附錄，以瞭解有關rACL和GSR上接收路徑流量的其他詳細資訊。

GSR有多個資料路徑，每個路徑都服務於不同形式的流量。傳輸流量從輸入線路卡(LC)轉送到交換矩陣，然後轉送到輸出卡，以進行下一個躍點遞送。除了中轉流量資料路徑之外，GSR還有另外兩條路徑用於需要本地處理的流量：LC到LC CPU，LC到LC CPU到交換矩陣到GRP。下表顯示了幾個常用功能和協定的路徑。

流量型別	資料路徑

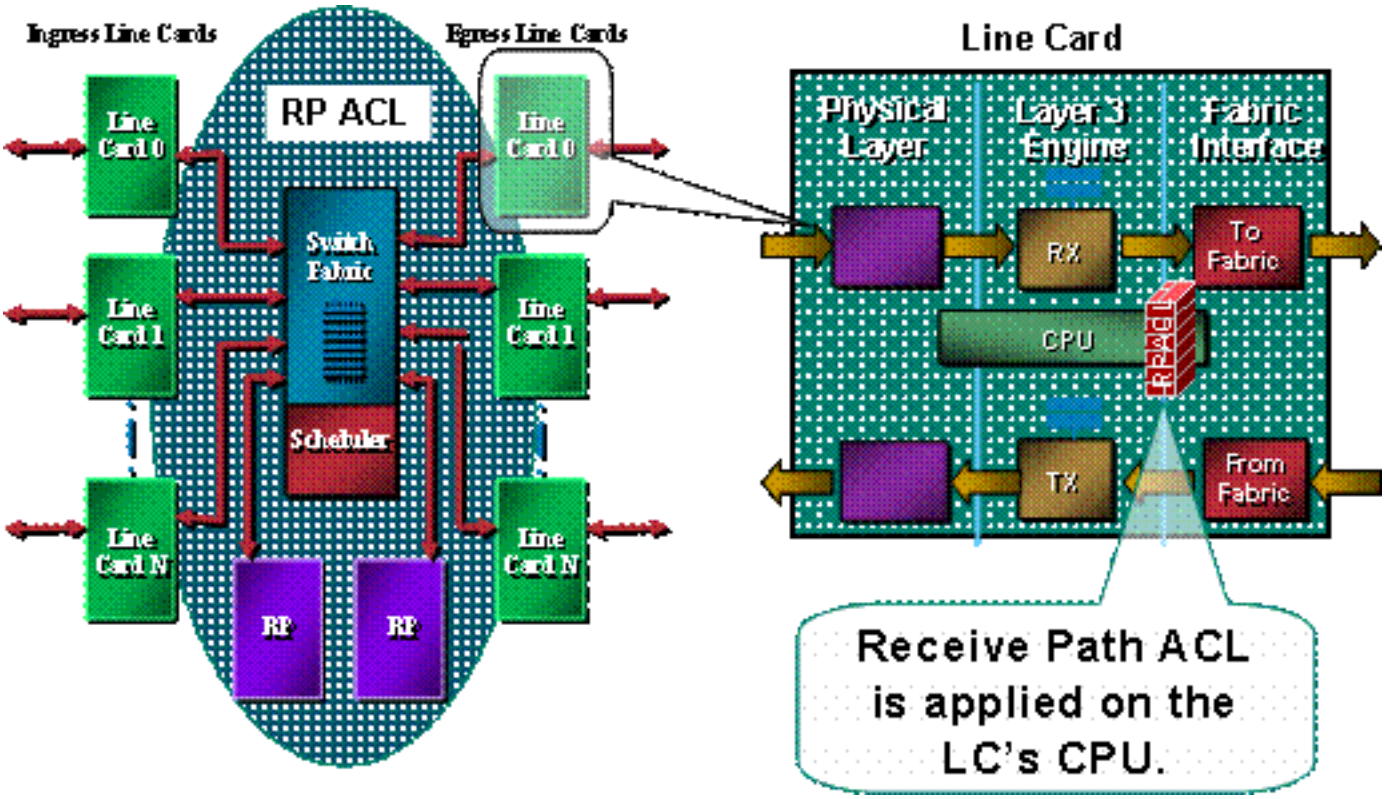
正常（傳輸）流量	LC到交換矩陣到LC
路由通訊協定/SSH/SNMP	LC到LC CPU到交換矩陣到GRP
ICMP回應(ping)	LC到LC CPU
記錄	

GSR的路由處理器處理從LC傳送到GRP本身的流量的能力有限。如果大量資料需要向GRP傳送，則該流量可能超過GRP。這將導致有效的拒絕服務(DoS)攻擊。GRP的CPU努力跟上資料包檢查的步伐，並開始丟棄資料包，泛洪輸入保持隊列和選擇性資料包丟棄(SPD)隊列。[2] GSR應針對三種情況加以保護，這三種情況可能是針對路由器的GRP進行的DoS攻擊所導致的。

- 正常優先順序泛洪導致的路由協定資料包丟失
- 正常優先順序泛洪導致的管理會話（Telnet、安全外殼[SSH]、SNMP）資料包丟失
- 偽造的高優先順序泛洪導致的資料包丟失

在正常優先順序泛洪期間，路由協定資料的潛在丟失目前通過靜態分類和從LC發往GRP的流量速率限製得以緩解。不幸的是，這一方法有侷限性。如果攻擊通過多個LC傳輸，則對發往GRP的正常優先順序流量的速率限制不足以保證對高優先順序路由協定資料的保護。通過降低正常優先順序資料的丟棄閾值來提供此類保護，只會加劇正常優先順序泛洪造成的管理流量損失。

如下圖所示，在每個LC上執行rACL後，封包才會傳輸到GRP。



需要GRP的保護機制。rACL會影響由於接收鄰接關係而傳送到GRP的流量。接收鄰接是指標對發往路由器IP地址的流量（例如廣播地址或在路由器介面上配置的地址）的Cisco Express Forwarding鄰接。[3] 請參閱附錄部分以瞭解更多有關接收鄰接和轉發資料包的詳細資訊。

進入LC的流量首先被傳送到LC的本地CPU，需要由GRP處理的資料包被排隊，以轉發到路由處理器。接收ACL在GRP上建立，然後向下推送到各個LC的CPU。流量從LC CPU傳送到GRP之前，先將流量與rACL進行比較。如果允許，流量會傳遞到GRP，而所有其他流量會遭到拒絕。在LC執行GRP速率限制功能之前檢查rACL。由於rACL用於所有接收鄰接，因此LC CPU處理的一些資料包（例如回應請求）也受到rACL過濾的影響。設計rACL條目時需要考慮這一點。

接收ACL是保護路由器中資源的多部分程式範圍機制的一部分。未來的工作將包括對rACL的速率限制元件。

效能影響

除了儲存單個配置條目和定義的訪問清單本身所需的記憶體之外，不佔用任何記憶體。rACL會複製到每個LC上，因此每個LC上會佔用一小部分記憶體。總體而言，使用的資源非常少，與部署收益相比尤其如此。

接收ACL不會影響轉發流量的效能。rACL僅適用於接收鄰接流量。轉送的流量從來不受rACL的制約。傳輸流量使用介面ACL進行過濾。這些「常規」 ACL應用於指定方向的介面。流量在rACL處理之前需要進行ACL處理，因此介面ACL拒絕的流量不會被rACL接收。[4]

由於rACL的處理，執行實際過濾的LC（換句話說，接收由rACL過濾的流量的LC）的CPU利用率將會增加。然而，CPU使用率的增加是由於發往GRP的大量流量造成的；rACL保護的GRP的好處遠遠超過增加LC上的CPU利用率。LC上的CPU利用率將因LC引擎型別而異。例如，給定相同的攻擊，引擎3 LC的CPU利用率將低於引擎0 LC。

啟用turbo ACL(使用**access-list compiled**命令)會將ACL轉換為一系列高效的查詢表條目。啟用增強型ACL後，rACL深度不會影響效能。換句話說，處理速度與ACL中的條目數量無關。如果rACL短，增強型ACL不會顯著提升效能，但會消耗記憶體；使用短rACL時，可能不需要編譯ACL。

通過保護GRP，rACL有助於確保路由器，並最終確保攻擊期間的網路穩定性。如上所述，rACL在LC CPU上處理，因此當大量資料指向路由器時，每個LC上的CPU利用率都會增加。在E0/E1和某些E2捆綁包上，100+%的CPU利用率可能導致路由協定和鏈路層丟棄。這些丟包已本地化，並且GRP路由進程受到保護，從而保持穩定性。在負載較重且僅將優先順序6和7流量轉發到路由協定時，啟用限制功能的E2卡[5]會啟用限制模式。其它引擎型別具有多隊列架構；例如，E3卡有三個到達CPU的隊列，路由協定資料包（優先順序6/7）位於一個單獨的高優先順序隊列中。高LC CPU，除非高優先順序資料包導致高優先順序，否則不會導致路由協定丟棄。到較低優先順序隊列的資料包將被尾部丟棄。最後，基於E4的卡有8個到CPU的隊列，其中一個隊列專用於路由協定資料包。

語法

接收ACL與以下全域性配置命令一起應用，以將rACL分配到路由器中的每個LC。

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

在此語法中，*<num>*的定義如下。

```
<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

為了能夠使用此命令，您需要定義一個訪問清單，以標識應該允許與路由器通訊的流量。存取清單需要包括路由通訊協定和管理流量（邊界閘道通訊協定[BGP]、開放最短路徑優先[OSPF]、SNMP、SSH、Telnet）。 有關詳細資訊，請參閱部署指南一節。

以下示例ACL提供了一個簡單的大綱，並提供了一些適用於特定用途的配置示例。ACL說明了幾種常用服務/協定所需的配置。對於SSH、Telnet和SNMP，使用環回地址作為目標。對於路由協定，使用實際介面地址。在rACL中使用的路由器介面選擇取決於本地站點策略和操作。例如，如果回送用於所有BGP對等作業階段，則在BGP的**permit**陳述式中，只需允許那些回送。

```
!--- 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
```

與所有Cisco ACL一樣，存取清單的結尾都有一個隱含的**deny**陳述式，因此與ACL中的專案不匹配的任何流量都會遭到拒絕。

注意：**log**關鍵字可用於幫助對目的地為不允許的GRP的流量進行分類。雖然**log**關鍵字提供了有關ACL命中詳細資訊的寶貴見解，但使用此關鍵字的過多命中ACL條目將增加LC CPU利用率。與記錄相關的效能影響將因LC引擎型別而異。一般情況下，只有在引擎0/1/2上必要時才使用日誌記錄。對於引擎3/4/4+，日誌記錄產生的影響要小得多，因為CPU效能提高和多隊列體系結構更好。

此訪問清單的粒度級別由本地安全策略決定（例如，OSPF鄰居所需的過濾級別）。

rACL和分段的資料包

ACL有一個**fragments**關鍵字，用於啟用專門的分段封包處理行為。通常，與ACL中的L3語句（不考慮L4資訊）匹配的非初始片段會受到匹配條目的**permit**或**deny**語句的影響。請注意，使用**fragments**關鍵字可強制ACL以更細緻的方式拒絕或允許非初始片段。

在rACL上下文中，過濾片段會針對僅使用非初始片段（例如FO > 0）的DoS攻擊新增額外的保護層。 在rACL的開頭對非初始片段使用**deny**語句可拒絕所有非初始片段訪問路由器。在極少數情況下，有效會話可能需要分段，因此如果rACL中存在**deny fragment**語句，則會對其進行過濾。

例如，請考慮以下所示的部分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>
```

將這些條目新增到rACL的開頭會拒絕任何非初始片段訪問GRP，而未分段的資料包或初始片段會傳遞到rACL的下一行，而不受**deny fragment**語句影響。上述rACL片段也有助於對攻擊進行分類，因為通用資料包通訊協定(UDP)、TCP和ICMP等每個通訊協定都會增加ACL中的獨立計數器。

請參閱存取控制清單和IP片段，以取得選項的詳細討論。

風險評估

確保rACL不會過濾關鍵流量，例如路由協定或對路由器的互動式訪問。過濾必要的流量可能導致無法遠端訪問路由器，因此需要控制檯連線。因此，實驗配置應儘可能模擬實際部署。

與往常一樣，思科建議您在部署之前在實驗室中測試此功能。

附錄和註釋

接收鄰接和轉發資料包

如本文檔前面所述，某些資料包需要GRP處理。資料包從資料轉發平面轉發到GRP。這是需要GRP訪問的第3層資料的常見形式清單。

- 路由協定
- 多點傳送控制流量（OSPF、熱待命路由器通訊協定[HSRP]、標籤分佈通訊協定[TDP]、通訊協定無關多點傳送[PIM]等）
- 需要分段的多重通訊協定標籤交換(MPLS)封包
- 具有某些IP選項（例如路由器警報）的資料包
- 組播流的第一個資料包
- 需要重組的分段ICMP資料包
- 所有目的地為路由器本身的流量（LC上處理的流量除外）

由於rACL應用於接收鄰接，因此rACL會過濾一些未傳送到GRP但屬於接收鄰接的流量。最常見的例子是ICMP回應請求(ping)。導向路由器的ICMP回應請求由LC CPU處理；由於請求是接收鄰接關係，因此也會通過rACL進行過濾。因此，要允許對路由器的介面（或環回）執行ping，rACL必須明確允許回應請求。

可以使用**show ip cef**命令檢視接收鄰接。

```
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

思科建議採用保守的部署做法。要成功部署rACL，必須充分瞭解現有的控制和管理平面訪問要求。在某些網路中，確定構建過濾清單所需的準確流量配置檔案可能比較困難。以下准則介紹了使用迭代rACL配置部署rACL的非常保守的方法，以幫助識別並最終過濾流量。

1. **使用分類ACL識別網路中使用的協定。**部署允許所有已知協定訪問GRP的rACL。此「發現」rACL應將源和目標地址都設定為**any**。日誌記錄可用於生成與協定**permit**語句匹配的源地址清單。除**permit**語句外，還可使用rACL末尾的**permit any any log**行來標識將由rACL過濾並可能需要訪問GRP的其他協定。目標是確定特定網路使用哪些協定。應使用日誌記錄進行分析，以確定可能與路由器通訊的「其他內容」。**注意：雖然log關鍵字提供了關於ACL命中詳細資訊**

的寶貴見解，但使用此關鍵字的ACL條目如果命中過多，可能會導致日誌條目數量過多，並且路由器CPU使用率可能很高。僅在需要幫助分類流量時，才短期使用log關鍵字。

2. **檢視確定的資料包並開始過濾對GRP的訪問。**在識別並檢查了步驟1中由rACL過濾的資料包後，為允許的協定部署帶有permit any any語句的rACL。與步驟1一樣，log關鍵字可以提供與允許專案相符的封包的詳細資訊。在結尾使用deny any any log可幫助識別任何目的地為GRP的意外資料包。此rACL將提供基本保護，並允許網路工程師確保所有所需流量都得到允許。目的是測試在沒有IP源地址和目的地址明確範圍的情況下需要與路由器通訊的協定範圍。
3. **限制源地址的宏範圍。**僅允許將您分配的無類域間路由(CIDR)塊的整個範圍作為源地址。例如，如果已為您的網路分配了171.68.0.0/16，則僅允許來自171.68.0.0/16的源地址。此步驟可降低風險，而不會中斷任何服務。它還提供來自您的CIDR塊外部的可能訪問您裝置的裝置/人員的資料點。所有外部地址將被丟棄。外部BGP對等體將需要一個例外，因為會話允許的源地址將位於CIDR塊之外。此階段可能會保留幾天，以收集下一階段縮小rACL的資料。
4. **將rACL permit語句縮小為僅允許已知的授權源地址。**將源地址日益限製為僅允許與GRP通訊的源。
5. **限制rACL上的目的地位址。(*可選*)**某些Internet服務提供商(ISP)可能選擇僅允許特定協定使用路由器上的特定目的地址。此最後階段旨在限制接受協定流量的目的地址範圍。[6]

部署示例

以下示例顯示基於以下地址保護路由器的接收ACL。

- ISP的地址塊是169.223.0.0/16。
- ISP的基礎架構塊是169.223.252.0/22。
- 路由器的環回地址為169.223.253.1/32。
- 路由器是核心主幹路由器，因此只有內部BGP會話處於活動狀態。

根據此資訊，初始接收ACL可能與以下範例類似。由於我們知道基礎結構地址塊，因此我們首先允許整個地址塊。稍後，將會新增更詳細的訪問控制條目(ACE)，因為需要訪問路由器的所有裝置都將獲得特定地址。

```
!
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
```

備註

1. 請參閱瞭解選擇性封包捨棄(SPD)SPD和保留佇列原則以增加DoS抵抗力。
2. 有關思科快速轉發和鄰接的詳細資訊，請參閱思科快速轉發概述。
3. 有關ACL部署指南和相關命令的詳細討論，請參閱在Cisco 12000系列Internet路由器上實施ACL。
4. 這涉及Vanilla、邊界網關協定策略記帳(BGPPA)、每個介面速率控制(PIRC)和幀中繼流量管制(FRTP)捆綁包。
5. 接收路徑保護的第II階段將允許建立管理介面，自動限制哪個IP地址將偵聽傳入資料包。

相關資訊

- 存取清單支援頁面
- 技術支援 - Cisco Systems