設定和篩選IP存取清單

目錄

簡介

本檔案介紹各種型別的IP存取控制清單(ACL)及其如何過濾網路流量。

必要條件

需求

本文件沒有特定先決條件。所討論的概念存在於 Cisco IOS® 軟體版本 8.3 或更高版本中。每個存取清單功能下方都會註明這一點。

採用元件

本文件將討論各種類型的 ACL。其中一些自 Cisco IOS 軟體版本 8.3 就已存在，其他則是在之後的軟體版本中導入。每個類型的討論中都會註明這一點。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需檔案慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

本文件將說明 IP 存取控制清單 (ACL) 如何過濾網路流量。其中也包含 IP ACL 類型、功能可用性和網路中使用範例的簡短說明。

> **附註**：RFC 1700 包含已指派的公認連線埠號碼。RFC 1918包含私人網際網路的位址分配，也就是通常不得在網際網路上看到的IP位址。

> **附註**：只有註冊的思科使用者才能訪問內部資訊。

> **附註**：ACL也可用於定義流量到網路位址轉譯(NAT)、加密或過濾非IP通訊協定（例如AppleTalk或IPX）。這些功能的討論不在本文件的範圍之內。

ACL 概念

遮罩

遮罩會與IP ACL中的IP位址一起使用，指定必須允許和拒絕的專案。掩碼用於在介面上配置IP地址，其開頭為255，左邊值較大，例如IP地址10.165.202.129（掩碼為255.255.255.224）。IP ACL的遮罩則相反，例如遮罩0.0.0.255。這有時稱為反向遮罩或萬用字元遮罩。遮罩的值細分為二進位（0和1）時，結果可判斷處理流量時要考慮哪些的位址位元。0 表示必須考慮位址位元（完全符合）;遮罩中的1表示*不比對*。下表進一步說明了此概念。

遮罩範例	
網路位址（要處理的流量）	*10.1.1.0*
遮罩	*0.0.0.255*
網路位址（二進位）	*00001010.00000001.00000001.00000000*
遮罩（二進位）	*00000000.00000000.00000000.11111111*

根據二進位遮罩，您可以看到前三組（八位元）必須完全符合指定的二進位網路位址(00001010.00000001.00000001)。 最後一組數字*不比對*(.11111111)。 因此，所有以10.1.1開頭的流量都會符合，因為最後一個八位元*不比對*。因此，使用此遮罩會處理 10.1.1.1 到 10.1.1.255 (10.1.1.x) 的網路位址。

從 255.255.255.255 減去一般遮罩即可判斷 ACL 反向遮罩。在此範例中，是透過一般遮罩 255.255.255.0 來判斷網路位址 172.16.1.0 的反向遮罩。

- 255.255.255.255 - 255.255.255.0（一般遮罩）= 0.0.0.255（反向遮罩）

請注意ACL對等專案。

- 0.0.0.0/255.255.255.255的來源/萬用字元代表**任意。**
- 10.1.1.2/0.0.0.0的來源/萬用字元與主機**10.1.1.2**相同。

ACL 摘要

> **附註**：子網路遮罩也可以透過固定長度標記法來表示。例如，192.168.10.0/24 表示 192.168.10.0 255.255.255.0。

以下清單說明如何將一個範圍的網路總結到單一網路中，以進行 ACL 最佳化。請考慮使用這些網路。

```
192.168.32.0/24
192.168.33.0/24
192.168.34.0/24
192.168.35.0/24
192.168.36.0/24
192.168.37.0/24
192.168.38.0/24
192.168.39.0/24
```

每個網路的前兩個八位元和最後一個八位元都相同。下表說明如何將這些網路總結到單一網路中。

可以將以上網路的第三個八位元寫成如下表所示，對應於每個位元的八位元位置和位址值。

十進位	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	D	D	D

因為前五個位元都相符，因此上述的八個網路可以總結成單一網路（192.168.32.0/21 或 192.168.32.0 255.255.248.0）。 三個低位位元的所有八種可能組合都與上述網路範圍相關。以下命令可定義允許此網路的 ACL。如果從 255.255.255.255 減去 255.255.248.0（一般遮罩），就會得出 0.0.7.255。

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

請考慮使用以下網路以取得更多說明。

```
192.168.146.0/24
192.168.147.0/24
192.168.148.0/24
192.168.149.0/24
```

每個網路的前兩個八位元和最後一個八位元都相同。下表說明如何總結這些網路。

可以將以上網路的第三個八位元寫成如下表所示，對應於每個位元的八位元位置和位址值。

十進位	128	64	32	16	8	4	2	1
146	1	0	0	1	0	0	1	0
147	1	0	0	1	0	0	1	1
148	1	0	0	1	0	1	0	0
149	1	0	0	1	0	1	0	1
	M	M	M	M	M	?	?	?

與先前的範例不同，您不能將這些網路總結到單一網路中。如果將這些網路總結到單一網路，它們會變成 192.168.144.0/21，因為第三個八位元中有五個位元相似。這個總結後的網路192.168.144.0/21涵蓋從192.168.144.0到192.168.151.0的一系列網路。其中，192.168.144.0、192.168.145.0、192.168.150.0和192.168.151.0網路不在指定的四個網路清單中。若要涵蓋相關的特定網路，您至少需要兩個總結的網路。指定的四個網路可以總結到這兩個網路中：

- 對於網路192.168.146.x和192.168.147.x，除了最後一個位元(也就是*不比對)之外，所有位元都相符*。因此可以寫為 192.168.146.0/23（或 192.168.146.0 255.255.254.0）。
- 對於網路192.168.148.x和192.168.149.x，除了最後一個位元(也就是*不比對)之外，所有位元都相符*。因此可以寫為 192.168.148.0/23（或 192.168.148.0 255.255.254.0）。

以下輸出定義了上述網路的總結ACL。

```
!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.146.0 to 192.168.147.254. access-list 10 permit
192.168.146.0 0.0.1.255
```

```
!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.148.0 to 192.168.149.254 access-list 10 permit
192.168.148.0 0.0.1.255
```

處理 ACL

進入路由器的流量會根據項目在路由器中發生的順序與 ACL 項目進行比較。新陳述式會新增到清單的結尾。路由器會繼續查看直到找到相符項目。如果路由器到達清單結尾時未找到相符項目，則會拒絕流量。因此，您必須在清單頂部列出經常命中的專案。對於不允許的流量有一個隱含的 deny。只有一個deny專案的單一專案ACL可以拒絕所有流量。ACL 中必須至少有一個 permit 陳述式，否則所有流量都會遭到封鎖。以下兩個 ACL（101 和 102）具有相同的效果。

```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected. access-list 101 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255


!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected. access-list 102 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

在下一個示例中，最後一個條目就足夠了。您不需要前三個專案，因為IP包括TCP、使用者資料包通訊協定(UDP)和網際網路控制訊息通訊協定(ICMP)。

```
!--- This command is used to permit Telnet traffic
!--- from machine 10.1.1.2 to machine 172.16.1.1. access-list 101 permit tcp host 10.1.1.2 host
172.16.1.1 eq telnet


!--- This command is used to permit tcp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine. access-list 101 permit tcp host 10.1.1.2
host 172.16.1.1


!--- This command is used to permit udp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine. access-list 101 permit udp host 10.1.1.2
host 172.16.1.1


!--- This command is used to permit ip traffic from
!--- 10.1.1.0 network to 172.16.1.10 network. access-list 101 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
```

定義連接埠和訊息類型

您不僅可以定義ACL來源和目的地，還可以定義連線埠、ICMP訊息型別和其他引數。若要瞭解公認連接埠的資訊，請參閱 RFC 1700 。如需 ICMP 訊息類型的說明，請參閱 RFC 792 。

路由器可以顯示一些公認連接埠的描述性文字。使用**a?可**獲得幫助。

```
access-list 102 permit tcp host 10.1.1.1 host 172.16.1.1 eq ?
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
```

設定期間，路由器也會將數值轉換為易於使用的值。在以下範例中，輸入ICMP訊息型別編號，就會使路由器將數字轉換為名稱。

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 14
```

變成

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 timestamp-reply
```

套用 ACL

您可以定義ACL，但無需套用。但是，在將 ACL 套用至路由器的介面之前，ACL 不會有任何作用。將 ACL 套用到距離流量來源最近的介面是很好的作法。如以下範例所示，當您嘗試封鎖從來源到目的地的流量時，可以將傳入ACL套用到路由器A的E0，而不是將傳出清單套用到路由器C的E1。存取清單在任何存取清單的結尾都隱含有**deny ip any** any。如果流量與DHCP要求相關，且並未明確允許，則該流量會遭到捨棄，因為當您檢視IP中的DHCP要求時，來源位址為s=0.0.0.0(Ethernet1/0),d=255.255.255.255,len 604,rcvd 2 UDP src=68,dst=67。請注意，來源IP位址為0.0.0.0，目的地位址為255.255。來源連線埠為8和目的地67。因此，您必須在存取清單中允許此類流量，否則流量會因為語句結尾的隱含deny而遭到捨棄。

附註：若要讓UDP流量通過，也必須由ACL明確允許UDP流量。

定義內送、外寄、傳入、傳出、來源和目的地

路由器會使用內送、外寄、來源和目的地等術語作為參照。路由器上的流量可比喻為高速公路上的交通。如果您是賓州的執法人員，且想要擋下一輛從馬里蘭到紐約的卡車，則卡車的來源就是馬里蘭，目的地則是紐約。路障可設定在賓州和紐約邊界（外寄）或馬里蘭和賓州邊界（內送）。

提及路由器時，這些術語則具有以下意義。

- **外寄 — 已通過路由器且離開介面的流量。**來源是指它原本在路由器另一端的位置，目的地則是它要前往的位置。
- **內送 — 到達介面並通過路由器流量。**來源是指它原本的位置，目的地則是它在路由器另一端要前往的位置。
- **傳入 — 如果存取清單為傳入，則當路由器收到封包時，Cisco IOS 軟體會檢查存取清單的條件陳述式是否有相符項目。**如果該封包允許通過，軟體將繼續處理該封包。如果該封包遭到拒絕，軟體將捨棄該封包。
- **傳出 — 如果存取清單為傳出，則在軟體收到封包並將其路由到傳出介面後，軟體會檢查存取清單的條件陳述式是否有相符項目。**如果該封包允許通過，軟體將傳送該封包。如果該封包遭到拒絕，軟體將捨棄該封包。

內送 ACL 的來源是在其套用的目標介面區段上，目的地則是在任何其他介面上。外寄 ACL 的來源是在其套用之介面以外的任何介面區段上，目的地則是在所套用的介面上。

編輯 ACL

編輯 ACL 時需要特別注意。例如，如果您打算從如下所示的編號 ACL 中刪除特定行，則系統會刪除整個 ACL。

```
!--- The access-list 101 denies icmp from any to any network
!--- but permits IP traffic from any to any network. router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
```

```
router(config)#access-list 101 deny icmp any any
router(config)#access-list 101 permit ip any any
router(config)#^Z

router#show access-list
Extended IP access list 101
    deny icmp any any
    permit ip any any
router#
*Mar  9 00:43:12.784: %SYS-5-CONFIG_I: Configured from console by console

router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#no access-list 101 deny icmp any any
router(config)#^Z

router#show access-list
router#
*Mar  9 00:43:29.832: %SYS-5-CONFIG_I: Configured from console by console
```

將路由器的組態複製到 TFTP 伺服器或記事本等文字編輯器中，即可編輯編號的 ACL。然後進行任何變更，並將組態複製回路由器。

您也可以執行以下操作。

```
router#configure terminal
  Enter configuration commands, one per line.
  router(config)#ip access-list extended test

!--- Permits IP traffic from 10.2.2.2 host machine to 10.3.3.3 host machine. router(config-ext-
nacl)#permit ip host 10.2.2.2 host 10.3.3.3

!--- Permits www traffic from 10.1.1.1 host machine to 10.5.5.5 host machine. router(config-ext-
nacl)#permit tcp host 10.1.1.1 host 10.5.5.5 eq www

!--- Permits icmp traffic from any to any network. router(config-ext-nacl)#permit icmp any any

!--- Permits dns traffic from 10.6.6.6 host machine to 10.10.10.0 network. router(config-ext-
nacl)#permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
  router(config-ext-nacl)#^Z
  1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

  router#show access-list
  Extended IP access list test
      permit ip host 10.2.2.2 host 10.3.3.3
      permit tcp host 10.1.1.1 host 10.5.5.5 eq www
      permit icmp any any
      permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
```

所有刪除內容都將從 ACL 中移除，任何新增項目則是會新增到 ACL 結尾。

```
router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#ip access-list extended test

!--- ACL entry deleted. router(config-ext-nacl)#no permit icmp any any

!--- ACL entry added. router(config-ext-nacl)#permit gre host 10.4.4.4 host 10.8.8.8
   router(config-ext-nacl)#^Z
   1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

   router#show access-list
```

```
   Extended IP access list test
       permit ip host 10.2.2.2 host 10.3.3.3
       permit tcp host 10.1.1.1 host 10.5.5.5 eq www
       permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
       permit gre host 10.4.4.4 host 10.8.8.8
```

您也可以依照 Cisco IOS 中的序號將 ACL 行新增到編號的標準型或編號的延伸型 ACL 。以下是組態範例：

請透過以下方式設定延伸型 ACL：

```
Router(config)#access-list 101 permit tcp any any
Router(config)#access-list 101 permit udp any any
Router(config)#access-list 101 permit icmp any any
Router(config)#exit
Router#
```

發出show access-list命令以檢視ACL專案。這裡也顯示了 10、20 和 30 等序號。

```
Router#show access-list
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

為存取清單 101 新增序號為 5 的項目。

範例 1：

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#5 deny tcp any any eq telnet
Router(config-ext-nacl)#exit
Router(config)#exit
Router#
```

在show access-list命令輸出中，序號5的ACL會新增為存取清單101的第一個專案。

```
Router#show access-list
Extended IP access list 101
    5 deny tcp any any eq telnet
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
Router#
```

範例 2：

```
internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any

internetrouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
internetrouter(config)#ip access-list extended 101
```

```
internetrouter(config-ext-nacl)#18 per tcp any host 172.16.2.11
internetrouter(config-ext-nacl)#^Z

internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    18 permit tcp any host 172.16.2.11
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any
internetrouter#
```

同樣地，您可以透過以下方式設定標準型存取清單：

```
internetrouter(config)#access-list 2 permit 172.16.1.2
internetrouter(config)#access-list 2 permit 172.16.1.10
internetrouter(config)#access-list 2 permit 172.16.1.11

internetrouter#show access-lists
Standard IP access list 2
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    10 permit 172.16.1.2

internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#25 per 172.16.1.7
internetrouter(config-std-nacl)#15 per 172.16.1.16

internetrouter#show access-lists
Standard IP access list 2
    15 permit 172.16.1.16
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    25 permit 172.16.1.7
    10 permit 172.16.1.2
```

標準型存取清單的主要差異在於Cisco IOS會依照IP位址的後續順序新增專案，而不是依照序號。

以下範例顯示了不同的項目，例如，如何允許 IP 位址 (192.168.100.0) 或網路 (10.10.10.0)。

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
    19 permit 10.101.110.0, wildcard bits 0.0.0.255
    25 deny any
```

在存取清單 2 中新增項目以允許 IP 位址 172.22.1.1：

```
internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#18 permit 172.22.1.1
```

此項目會新增到清單頂端，以便為特定 IP 位址（而不是網路）提供優先順序。

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    18 permit 172.22.1.1
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
```

```
19 permit 10.101.110.0, wildcard bits 0.0.0.255
25 deny   any
```

附註：ASA/PIX 防火牆等安全設備不支援先前的 ACL。

將存取清單套用到密碼編譯對應後變更存取清單的準則

- 如果對目前的存取清單組態新增內容，就不需要移除密碼編譯對應。如果在未移除密碼編譯對應的情況下直接新增內容，則此操作會受到支援而且是可接受的。
- 如果需要從目前存取清單中修改或刪除存取清單專案，則必須從介面移除密碼編譯對應。刪除密碼編譯對應後，請對存取清單進行所有變更並重新新增密碼編譯對應。如果在未移除密碼編譯對應的情況下進行變更（例如刪除存取清單），則此操作不會受到支援，而且可能會導致不可預測的行為。

疑難排解

如何從介面中移除 ACL？

若要將 ACL 從介面中移除，請進入組態模式，然後在 access-group 命令前方輸入 **no，如以下範例所示。**

```
interface <interface-name> no ip access-group <acl-number> {in|out}
```

遭到拒絕的流量過多時，該怎麼做？

如果遭到拒絕的流量過多，請研究您的清單邏輯，或嘗試定義並套用其他更廣泛的清單。**show ip access-lists 命令會提供一個封包數量，顯示所命中的 ACL 項目。**除了連接埠特定的資訊以外，個別 ACL 項目結尾的 log 關鍵字還會顯示 ACL 編號以及封包允許通過或遭到拒絕。

附註：log-input 關鍵字存在於 Cisco IOS 軟體版本 11.2 和更高版本中，以及在特別為服務提供者建立的特定 Cisco IOS 軟體版本 11.1 型軟體中。舊版軟體不支援此關鍵字。此關鍵字的使用包括輸入介面和來源 MAC 位址（如果適用）。

如何在使用思科路由器的封包層級進行偵錯？

以下程序將說明偵錯流程。開始之前，請確定目前並未套用任何 ACL、已備妥一個 ACL，而且快速交換功能並未停用。

附註：對具有大量流量的系統進行偵錯時，請特別小心。使用 ACL 可對特定流量進行偵錯。但是要確保流程和流量。

1. 使用**access-lists**命令可擷取所需的資料。以下範例是針對目的地位址 10.2.6.6 或來源位址 10.2.6.6 設定資料擷取。
   ```
   access-list 101 permit ip any host 10.2.6.6
   access-list 101 permit ip host 10.2.6.6 any
   ```
2. 停用相關介面上的快速交換功能。如果快速交換功能未停用，您只會看到第一個封包。
   ```
   configure terminal
   ```

```
interface
```

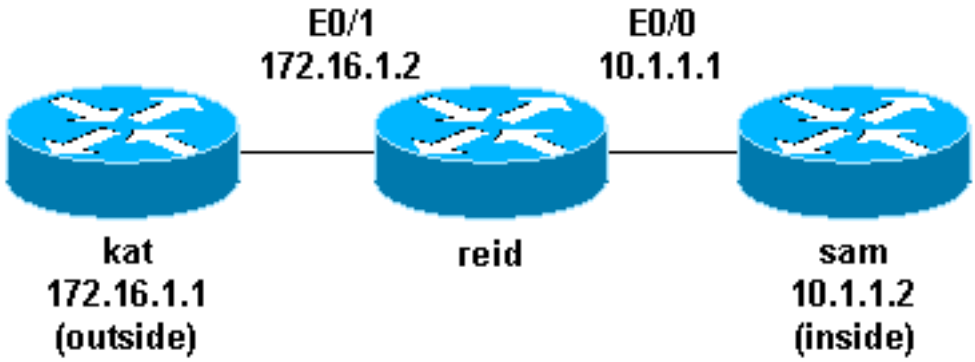
3. 在啟用模式下使用 **terminal monitor** 命令以顯示 debug 命令輸出以及目前終端和作業階段的系統錯誤訊息。
4. 使用**debug ip packet 101**或**debug ip packet 101 detail**命令以開始偵錯流程。
5. 在啟用模式下執行 **no debug all 命令和 interface configuration 命令可停止偵錯流程。**
6. 重新啟動快取。

```
configure terminal
interface
```

IP ACL 的類型

本文件的此節將說明 ACL 類型。

網路圖表



標準型 ACL

標準型 ACL 是最舊的 ACL 類型。它們可回溯至Cisco IOS軟體版本8.3。標準型ACL會將IP封包的來源位址與ACL中設定的位址進行比較，以便控制流量。

以下是標準型 ACL 的命令語法格式。

```
access-list <access-list-number> {permit|deny} {host|source source-wildcard|any}
```

在所有軟體版本中，*access-list-number*可以是1到99之間的任何數字。在Cisco IOS軟體版本12.0.1中，標準型ACL開始使用其他數字（1300到1999）。 這些額外的數字稱為延伸型 IP ACL。Cisco IOS 軟體版本 11.2 新增了在標準型 ACL 中使用清單 *name 的功能*。

0.0.0.0/255.255.255.255的*source/source-wildcard*設定可指定為**any**。如果全部都是零，則可以省略 wildcard。因此，主機10.1.1.2 0.0.0.0與主機10.1.1.2相同。

定義 ACL 後，必須將其套用至介面（傳入或傳出）。 在早期軟體版本中，如果未指定關鍵字 out 或 in 時，預設為 out。在更高的軟體版本中必須指定方向。

```
interface <interface-name>
 ip access-group number {in|out}
```

以下是使用標準型 ACL 封鎖來源 10.1.1 以外之所有流量的範例。

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 1 in
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

延伸型 ACL

延伸型ACL是在Cisco IOS軟體版本8.3中匯入。延伸型ACL會將IP封包的來源和目的地位址與ACL中設定的位址進行比較，以便控制流量。

以下是延伸型 ACL 的命令語法格式。為了空間考慮，此處會換行。

IP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} protocol source source-wildcard destination destination-wildcard [precedence
precedence]
     [tos tos] [log|log-input] [time-range time-range-name]
```

ICMP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} icmp source source-wildcard destination destination-wildcard
     [icmp-type [icmp-code] |icmp-message] [precedence precedence] [tos tos] [log|log-input]
     [time-range time-range-name]
```

TCP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} tcp source source-wildcard [operator [port]]
     destination destination-wildcard [operator [port]]
     [established] [precedence precedence] [tos tos]
     [log|log-input] [time-range time-range-name]
```

UDP

```
access-list access-list-number
     [dynamic dynamic-name [timeout minutes]]
     {deny|permit} udp source source-wildcard [operator [port]]
     destination destination-wildcard [operator [port]]
     [precedence precedence] [tos tos] [log|log-input]
     [time-range time-range-name]
```

在所有軟體版本中，*access-list-number*可以是100到199之間的任何數字。在Cisco IOS軟體版本12.0.1中，延伸型ACL開始使用其他數字（2000到2699）。 這些額外的數字稱為延伸型 IP ACL。Cisco IOS 軟體版本 11.2 新增了在延伸型 ACL 中使用清單 *name 的功能。*

您可以將 0.0.0.0/255.255.255.255 的值指定為 **any。**定義 ACL 後，必須將其套用至介面（傳入或傳出）。 在早期軟體版本中，如果未指定關鍵字 out 或 in 時，預設為 out。在更高的軟體版本中必須指定方向。

```
interface <interface-name>
 ip access-group {number|name} {in|out}
```

此延伸型ACL是用來允許10.1.1.x網路上的流量（內部），並從外部接收ping回應，同時防止外部人員未經請求的ping允許所有其他流量。

```
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group 101 in
!
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo access-list 101 permit ip any 10.1.1.0
0.0.0.255
```

> **附註**：某些應用程式（例如網路管理）需要 ping 才能執行 keepalive 功能。如果是這種情況，您可以限制已封鎖的傳入ping，或是更詳細指定允許/拒絕的IP。

鎖鑰型（動態 ACL）

鎖鑰型也稱為動態ACL，是在Cisco IOS軟體版本11.1中匯入。此功能須仰賴Telnet、驗證（本機或遠端）以及延伸型ACL。

鎖鑰型組態會從套用延伸型 ACL 開始，以阻擋流量通過路由器。想要在路由器周遊的使用者會遭到延伸型 ACL 封鎖，直到他們 Telnet 到路由器且經過驗證為止。接著，Telnet連線將會捨棄，而且系統會將單一專案動態ACL新增到現有的延伸型ACL中。這樣會在特定期間允許流量；可以設定閒置和絕對逾時。

以下是用於使用本機驗證之鎖鑰型組態的命令語法格式。

```
username <user-name> password <password>
!
interface <interface-name>
 ip access-group {number|name} {in|out}
```

此命令中的單一項目 ACL 會在驗證之後以動態方式新增到現有的 ACL 中。

```
access-list access-list-number dynamic name {permit|deny} [protocol]
{source source-wildcard|any} {destination destination-wildcard|any}
[precedence precedence][tos tos][established] [log|log-input]
[operator destination-port|destination port]

line vty <line_range>
login local
```

以下是鎖鑰型組態的基本範例。

```
username test password 0 test

!--- Ten (minutes) is the idle timeout. username test autocommand access-enable host timeout 10
!
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip access-group 101 in
!
access-list 101 permit tcp any host 10.1.1.1 eq telnet

!--- 15 (minutes) is the absolute timeout. access-list 101 dynamic testlist timeout 15 permit ip
10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
!
line vty 0 4
 login local
```

10.1.1.2 上的使用者建立與 10.1.1.1 的 Telnet 連線後，就會套用動態 ACL。接著，系統會捨棄該連線，使用者就可以前往 172.16.1.x 網路了。

IP 命名型 ACL

IP命名型ACL是在Cisco IOS軟體版本11.2中匯入。這樣可讓使用者為標準型和延伸型ACL指定名稱，而不是數字。

以下是 IP 命名型 ACL 的命令語法格式。

```
ip access-list {extended|standard} name
```

以下是 TCP 範例：

```
{permit|deny} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]] [established] [precedence precedence] [tos tos] [log] [time-range time-range-
name]
```

以下是使用命名型 ACL 來封鎖主機 10.1.1.2 到主機 172.16.1.1 之 Telnet 連線以外所有流量的範例。

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group in_to_out in
!
ip access-list extended in_to_out
 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

自反型 ACL

自反型ACL是在Cisco IOS軟體版本11.3中匯入。自反型ACL允許根據上層作業階段資訊來過濾IP封包。它們通常是用來允許傳出流量，以及限制傳入流量來回應源自路由器內部的作業階段。

自反型 ACL 只能透過延伸命名型 IP ACL 來定義，不能透過編號或標準命名型 IP ACL 或其他通訊

協定 ACL 來定義。自反型 ACL 可以和其他標準型及靜態延伸型存取清單結合使用。

以下是各種自反型 ACL 命令的語法。

```
interface <interface-name>
 ip access-group {number|name} {in|out}
!
ip access-list extended <name>
 permit protocol any any reflect name [timeoutseconds]
!
ip access-list extended <name>
 evaluate <name>
```

以下是允許ICMP傳出和傳入流量的範例，其中只允許從內部發出的TCP流量，其他流量將遭到拒絕。

```
ip reflexive-list timeout 120
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group inboundfilters in
 ip access-group outboundfilters out
!
ip access-list extended inboundfilters
 permit icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
 evaluate tcptraffic

!--- This ties the reflexive ACL part of the outboundfilters ACL,
!--- called tcptraffic, to the inboundfilters ACL. ip access-list extended outboundfilters
 permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
```

使用時間範圍的時間型 ACL

時間型 ACL 是在 Cisco IOS 軟體版本 12.0.1.T 中導入。雖然與作用中的延伸型 ACL 類似，但它們允許依照時間來進行存取控制。此時會建立一個時間範圍來定義特定日期和時間，以執行時間型 ACL。時間範圍是依照名稱識別，然後由函數參照。因此，時間限制會實施在函數本身。時間範圍取決於路由器系統時鐘。可以使用路由器時鐘，但該功能搭配網路時間協定 (NTP) 同步的效果最佳。

以下是時間型 ACL 命令。

```
!--- Defines a named time range. time-range time-range-name

!--- Defines the periodic times. periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm

!--- Or, defines the absolute times. absolute [start time date] [end time date]

!--- The time range used in the actual ACL. ip access-list name|number time-rangename_of_time-range
```

在此範例中，會在星期一、星期三和星期五的工作時間內允許從內部到外部網路的 Telnet 連線：

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
EVERYOTHERDAY
!
time-range EVERYOTHERDAY
 periodic Monday Wednesday Friday 8:00 to 17:00
```

備註型 IP ACL 項目

備註型 IP ACL 項目是在 Cisco IOS 軟體版本 12.0.2.T 中導入。備註會讓 ACL 更易於理解，而且可用於標準型或延伸型 IP ACL。

以下是加上備註的命名型 IP ACL 命令語法。

```
ip access-list {standard|extended} <access-list-name> remark remark
```

以下是加上備註的編號型 IP ACL 命令語法。

```
access-list <access-list-number> remark remark
```

以下是編號型ACL中的註釋範例。

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 remark permit_telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

內容型存取控制

內容型存取控制 (CBAC) 是在 Cisco IOS 軟體版本 12.0.5T 中導入，而且需要 Cisco IOS 防火牆功能集。CBAC 會檢查流經防火牆的流量，以發現和管理 TCP 和 UDP 作業階段的狀態資訊。此狀態資訊是用來在防火牆的存取清單中建立臨時入口。**在流量發起的方向設定ip** 檢查清單，以便為允許的作業階段（也就是源自受保護內部網路的作業階段）允許傳回流量和其他資料連線，即可完成上述作業。

以下是 CBAC 的語法。

```
ip inspect name inspection-name protocol [timeoutseconds]
```

以下是使用 CBAC 檢查傳出流量的範例。延伸型 ACL 111 通常會封鎖 ICMP 以外的傳回流量，而且沒有對傳回流量的 CBAC 開孔。

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw tcp timeout 3600
```

```
ip inspect name myfw udp timeout 3600
ip inspect name myfw tftp timeout 3600
! interface Ethernet0/1 ip address 172.16.1.2 255.255.255.0 ip access-group 111 in ip inspect
myfw out !
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo access-list 111 permit icmp any 10.1.1.0
0.0.0.255
```

驗證代理

驗證代理是在 Cisco IOS 軟體版本 12.0.5 中導入，會要求您設定 Cisco IOS 防火牆功能。驗證代理是用來對傳入和/或傳出使用者進行驗證。通常遭到 ACL 封鎖的使用者可以自備瀏覽器來通過防火牆，並在 TACACS+ 或 RADIUS 伺服器上進行驗證。伺服器會將其他 ACL 項目向下傳遞到路由器，以便在驗證之後允許使用者通過。

驗證代理類似於鎖鑰型（動態 ACL）。 以下是不同之處：

- 鎖鑰型是透過 Telnet 連線到路由器來開啟。驗證代理是由 HTTP 透過路由器來開啟。
- 驗證代理必須使用外部伺服器。
- 驗證代理可以處理多個動態清單的新增作業。鎖鑰型只能新增一個。
- 驗證代理具有絕對逾時，但沒有閒置逾時。鎖鑰型則兩者都有。

請參閱思科安全整合軟體組態秘笈以取得驗證代理的範例。

增強型 ACL

增強型 ACL 是在 Cisco IOS 軟體版本 12.1.5.T 中導入，而且僅能在 7200、7500 和其他高階平台上找到。增強型 ACL 功能旨在更有效地處理 ACL，以便提升路由器效能。

使用 **access-list compiled 命令可查看增強型 ACL。**以下是已編譯 ACL 的範例。

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp
```

定義標準型或延伸型 ACL 後，請使用 **global configuration 命令進行編譯。**

```
!--- Tells the router to compile. access-list compiled
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0

!--- Applies to the interface.  ip access-group 101 in
```

show access-list compiled 命令會顯示有關 ACL 的統計資料。

分散式時間型 ACL

分散式時間型 ACL 是在 Cisco IOS 軟體版本 12.2.2.T 中導入，以便在已啟用 VPN 的 7500 系列路由器上執行時間型 ACL。在導入分散式時間型 ACL 功能之前，Cisco 7500 系列路由器的線卡並不支援時間型 ACL。如果設定了時間型 ACL，它們的行為就與一般 ACL 相同。如果線卡上的介面設定了時間型 ACL，則交換到介面的封包不會透過線卡進行分散式交換，而是轉送到路由處理器以進行處理。

分散式時間型ACL的語法與時間型ACL的語法相同，還新增了路由處理器和線卡之間處理器間通訊(IPC)訊息之狀態相關的命令。

```
debug time-range ipc
show time-range ipc
clear time-range ipc
```

接收 ACL

接收 ACL 的使用目的是，透過防止路由器的 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 12.0(22)S 中。請參閱GSR:接收訪問控制列表以瞭解更多資訊。

基礎架構保護 ACL

基礎架構ACL的使用目的是，透過明確許可對基礎架構裝置的僅限授權流量，同時允許所有其他傳輸流量，以減少直接基礎架構攻擊所帶來的風險和有效性。請參閱保護您的核心：基礎架構保護存取控制清單以瞭解其他資訊。

傳輸 ACL

傳輸 ACL是用來提高網路資安，因為它們會明確允許只有所需的流量才能進入您的網路。請參閱傳輸存取控制清單：在邊緣進行過濾以瞭解詳細資訊。

相關資訊

- 設定常用的 IP ACL
- RFC 1700
- RFC 1918
- 存取清單支援頁面
- Cisco IOS 防火牆
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。