保護您的核心：基礎架構保護存取控制清單

目錄

簡介

本檔案介紹基礎架構保護存取控制清單(ACL)的准則和建議部署技術。 基礎架構ACL的使用目的是，透過明確允許只有授權流量才能到達基礎架構裝置，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。

基礎架構保護

背景

為了保護路由器免受各種風險（包括意外風險和惡意風險），應在網路入口點部署基礎設施保護ACL。這些IPv4和IPv6 ACL拒絕從外部源訪問所有基礎設施地址，例如路由器介面。同時，ACL允許常規傳輸流量不間斷地傳輸，並提供基本的RFC 1918 、RFC 3330 和反欺騙過濾。

路由器接收的資料可以分為兩大類：

- 通過轉發路徑的流量
- 通過接收路徑發往路由器的流量以進行路由處理器處理

在正常操作中，絕大部分流量只是通過路由器到達最終目的地。

但是，路由處理器(RP)必須直接處理某些型別的資料，最明顯的是路由協定、遠端路由器訪問（如安全外殼[SSH]）和網路管理流量(如簡單網路管理協定(SNMP))。 此外，諸如網際網路控制訊息通訊協定(ICMP)和IP選項等通訊協定可能需要RP進行直接處理。通常，僅需要從內部來源直接訪問基礎設施路由器。少數顯著的例外包括外部邊界閘道通訊協定(BGP)對等、在實際路由器上終止的通訊協定（例如通用路由封裝[GRE]或IPv6 over IPv4通道），以及可能用於連線測試的受限制

ICMP封包(例如回應要求或ICMP無法連線以及用於traceroute的存留時間(TTL)到期訊息。

注意：請記住，ICMP通常用於簡單的拒絕服務(DoS)攻擊，僅在必要時才允許來自外部來源的攻擊。

所有RP都有一個運行時的效能包絡。目的地為RP的流量過多可能會淹沒路由器。這會導致CPU使用率高，最終導致資料包和路由協定丟棄，從而導致拒絕服務。通過從外部來源過濾對基礎架構路由器的訪問，與直接路由器攻擊相關的許多外部風險得以緩解。外部來源攻擊不能再訪問基礎設施裝置。攻擊會在進入自治系統(AS)的入口介面上丟棄。

本文所述的過濾技術旨在過濾目的地為網路基礎架構裝置的資料。請勿將基礎設施過濾與通用過濾混淆。基礎架構保護ACL的唯一用途是在粒度級限制哪些協定和來源可以訪問關鍵基礎架構裝置。

網路基礎設施裝置包括以下方面：

- 所有路由器和交換機管理地址，包括環回介面
- 所有內部鏈路地址：路由器到路由器鏈路（點對點和多路訪問）
- 不應從外部源訪問的內部伺服器或服務

在本文檔中，所有不發往基礎設施的流量通常稱為中轉流量。

技術

可通過多種技術實現基礎架構保護：

- **接收ACL(rACL)**思科12000和7500平台支援過濾所有發往RP的流量且不影響傳輸流量的rACL。必須明確允許授權流量，並且必須在每台路由器上部署rACL。請參閱 GSR：接收存取控制清單以瞭解詳細資訊。
- **逐跳路由器ACL**通過定義ACL也可以保護路由器，這些ACL僅允許授權流量到達路由器介面，拒絕傳輸流量以外的所有其它流量，傳輸流量必須明確允許。此ACL在邏輯上與rACL類似，但會影響傳輸流量，因此可能會對路由器的轉發速率產生負面影響。
- **通過基礎架構ACL進行邊緣過濾**ACL可以應用到網路邊緣。對於服務提供商(SP)，這是AS的邊緣。此ACL會明確過濾目的地為基礎架構位址空間的流量。部署邊緣基礎架構ACL需要明確定義您的基礎架構空間以及訪問此空間的必要/授權協定。ACL應用於所有面向外部的連線（例如對等連線、客戶連線等）上的網路入口。本文檔重點介紹邊緣基礎架構保護ACL的開發和部署。

ACL示例

這些IPv4和IPv6訪問清單提供了保護ACL中所需的典型條目的簡單而又真實的示例。這些基本ACL需要使用本地站點特定的配置詳細資訊進行自定義。在雙IPv4和IPv6環境中，都會部署兩個訪問清單。

IPv4範例

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-
```

```
list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses. access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic. access-list 110 permit ip any any
```

IPv6示例

IPv6訪問清單必須作為擴展的、命名訪問清單應用。

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !--- Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses. deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6 any any
```

附註： log關鍵字可用於提供有關給定協定的源和目標的其他詳細資訊。雖然此關鍵字提供了有關ACL命中詳細資訊的寶貴資訊，但是對使用log關鍵字的ACL條目的過度命中會增加CPU利用率。與日誌記錄相關的效能影響因平台而異。此外，使用log關鍵字會為與access-list語句匹配的資料包禁用思科快速轉發(CEF)交換。這些封包將改為快速交換。

開發保護ACL

一般來說，基礎架構ACL由四個部分組成：

- 特殊用途地址和反欺騙條目，這些條目拒絕非法來源和具有源地址且屬於您的AS內的資料包從外部來源進入AS**注意**：RFC 3330定義了可能需要過濾的IPv4特殊使用地址。RFC 1918定義了IPv4保留地址空間，該空間不是有效的網際網路源地址。RFC 3513定義了IPv6編址架構。RFC 2827 提供輸入篩選准則。
- 明確允許且來源為外部且目的地為基礎設施地址的流量
- **deny語**句用於所有其他外部來源流量到基礎設施地址
- **在通**往非基礎設施目的地的路由中，普通主幹流量的所有其他流量的permit語句

基礎架構ACL中的最後一行明確允許傳輸流量：**permit ip any any** for IPv4 and **permit ipv6 any any** for IPv6。此條目確保所有IP協定都允許通過核心，並且客戶可以繼續運行應用程式而不會出現問題。

開發基礎架構保護ACL的第一步是瞭解所需的協定。雖然每個站點都有特定的要求，但某些協定是通用部署的，必須理解。例如，需要明確允許外部對等點的外部BGP。需要直接訪問基礎設施路由器的任何其他協定也需要得到明確允許。例如，如果在核心基礎架構路由器上終止GRE通道，則還需要明確允許協定47(GRE)。同樣，如果在核心基礎架構路由器上終止IPv6 over IPv4隧道，則還需要顯式允許協定41(IPv6 over IPv4)。

分類ACL可用於幫助識別所需的協定。分類ACL由可發往基礎架構路由器的各種協定的**permit**語句組成。有關完整清單，請參閱Cisco IOS®軟體中支援的IP協定的附錄。使用**show access-list命令**顯示訪問控制條目(ACE)命中數的命令可以識別所需的協定。在為意外協定建立**permit**語句之前，必須調查和瞭解可疑或意外結果。

例如，此IPv4 ACL有助於確定是否需要允許GRE、IPsec(ESP)和IPv6通道（IP協定41）。

```
access-list 101 permit GRE any infrastructure_ips
```

```
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted.

access-list 101 permit ip any any

interface <int>
 ip access-group 101 in
```

此IPv6 ACL可用於確定是否需要允許GRE和IPsec(ESP)。

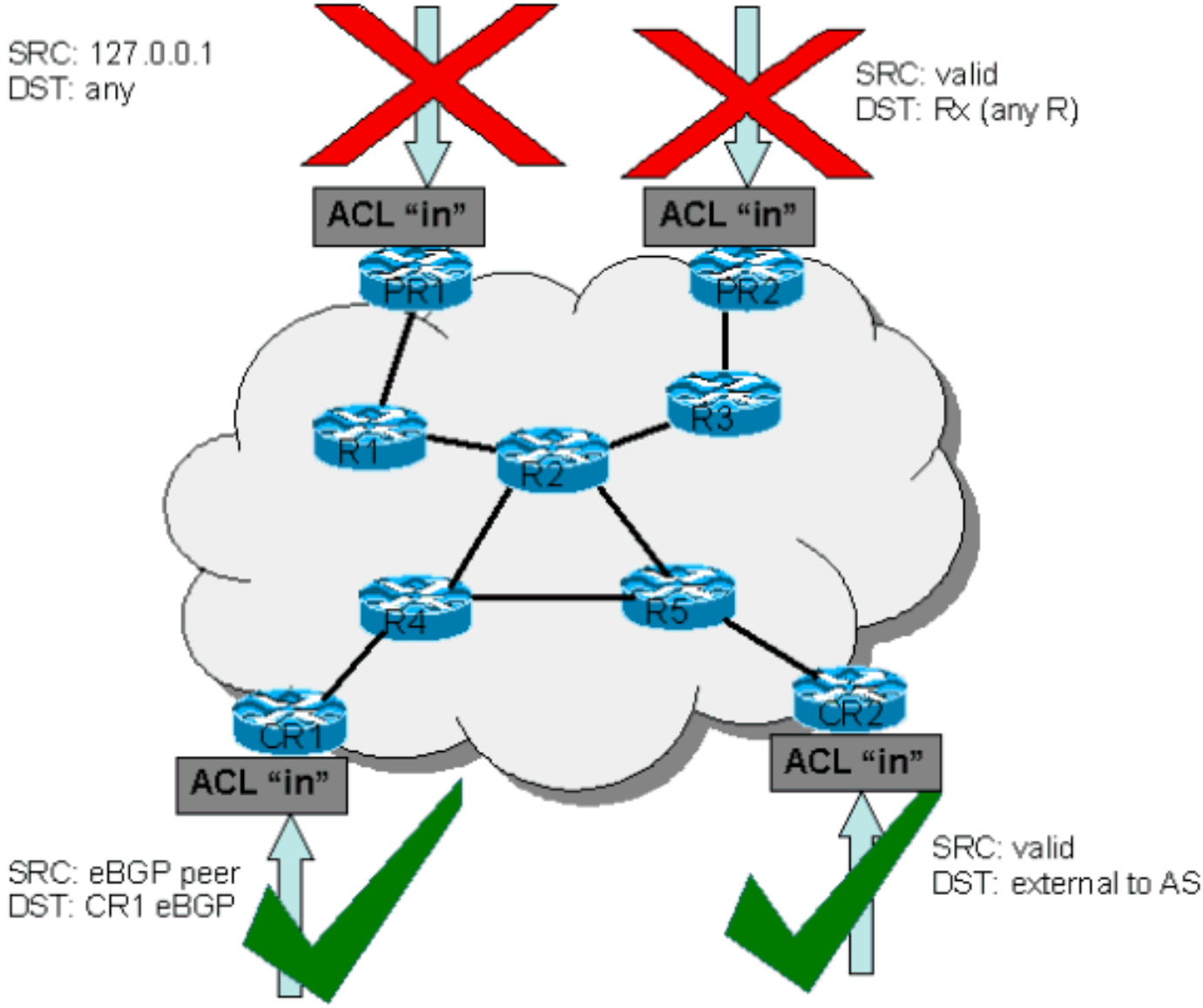
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

除所需的協定外，還需要標識基礎設施地址空間，因為這是ACL保護的空間。基礎架構地址空間包括用於內部網路且很少被外部來源（例如路由器介面、點對點鏈路定址和關鍵基礎架構服務）訪問的任何地址。由於這些地址用於基礎架構ACL的目標部分，因此總結至關重要。只要可能，這些地址必須分組到無類域間路由(CIDR)塊中。

使用確定的協定和地址後，可以構建基礎設施ACL來允許協定並保護地址。除了直接保護外，ACL還提供第一道防線，用於防範網際網路上特定型別的無效流量。

- 必須拒絕RFC 1918空間。
- 來源位址屬於特殊用途位址空間（如RFC 3330所定義）的資料包必須遭到拒絕。
- 必須應用反欺騙過濾器。（您的地址空間決不能是來自AS外部的資料包的來源。）

新構建的ACL必須應用於所有輸入介面的入站流量。有關詳細資訊，請參閱部署指南和部署示例上的部分。



ACL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。如果沒有**fragments**關鍵字，則與ACL中第3層語句（無論第4層資訊如何）匹配的非初始片段會受到匹配條目的permit或deny語句的影響。但是，通過新增**fragments**關鍵字，可以強制ACL以更高的粒度拒絕或允許非初始片段。IPv4和IPv6存取清單的此行為相同，不同之處在於，IPv4 ACL允許在第3層和第4層語句中使用fragments關鍵字，而IPv6 ACL僅允許在第3層語句中使用fragments關鍵字。

過濾片段為使用非初始片段（即FO > 0）的拒絕服務(DoS)攻擊新增額外的保護層。 在ACL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，有效作業階段可能需要分段，因此如果ACL中存在**deny fragment**陳述式，則會過濾有效作業階段。

例如，請考慮以下部分IPv4ACL:

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

將這些條目新增到ACL的開頭會拒絕對核心路由器的任何非初始分段訪問，而未分段的資料包或初始分段會傳遞到ACL的下一行，而不受**deny fragment**語句影響。前面的ACL命令也有助於對攻擊進

行分類，因為每個協定(通用資料包協定(UDP)、TCP和ICMP)都會增加ACL中的獨立計數器。

這是IPv6的一個類似示例：

```
ipv6 access-list iacl
   deny ipv6 any infrastructure_IP fragments
```

將此項新增到IPv6 ACL的開頭會拒絕任何對核心路由器的非初始分段訪問。如前所述，IPv6存取清單僅允許在第3層語句中使用fragments關鍵字。

由於許多攻擊依賴於向核心路由器泛洪分段資料包，因此將傳入片段過濾到核心基礎設施可提供額外的保護措施，並有助於確保攻擊無法僅通過匹配基礎設施ACL中的第3層規則來注入片段。

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

部署基礎設施保護ACL時，請考慮以下兩個關鍵風險：

- 確保具有適當的**permit/deny**語句。要使ACL生效，必須允許所有必需的協定，並且正確的地址空間必須由**deny**語句保護。
- ACL效能因平台而異。部署ACL之前，請先檢查硬體的效能特徵。

與往常一樣，建議您在部署之前在實驗室中測試此設計。

附錄

Cisco IOS軟體中支援的IP通訊協定

Cisco IOS軟體支援以下IP通訊協定：

- 1 - ICMP
- 2 - IGMP
- 3 - GGP
- 4 - IP內IP封裝
- 6 - TCP
- 8 - EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP
- 41 - IPv4隧道中的IPv6
- 46 - RSVP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 53 — 輕掃

- 54 - NARP
- 55 - IP移動性
- 63 — 任何本地網路
- 77 - Sun ND
- 80 - ISO IP
- 88 - EIGRP
- 89 - OSPF
- 90 - Sprite RPC
- 91 — 拉普
- 94 - KA9Q/NOS相容IP over IP
- 103 - PIM
- 108 - IP壓縮
- 112 - VRRP
- 113 - PGM
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

部署指南

思科建議採用保守的部署做法。為了成功部署基礎設施ACL，必須充分瞭解所需的協定，而且必須明確標識和定義地址空間。這些准則介紹了使用迭代法部署保護ACL的非常保守的方法。

1. **使用分類ACL識別網路中使用的協定。**部署允許訪問基礎設施裝置的所有已知協定的ACL。此發現ACL的源地址為**any**，目標地址包括基礎架構IP空間。日誌記錄可用於生成與協定**permit**語句匹配的源地址清單。要允許流量，需要允許**ip any any**(IPv4)或**ipv6 any any**(IPv6)的最後一條線路。目標是確定特定網路使用哪些協定。日誌記錄用於分析，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。**此外，使用**log**關鍵字會為與access-list語句匹配的資料包禁用思科快速轉發(CEF)交換。這些封包將改為快速交換。僅在需要幫助分類流量時，才短期使用**log**關鍵字。
2. **檢查識別的資料包並開始過濾對路由處理器RP的訪問。**在識別並檢查了步驟1中由ACL過濾的資料包後，請部署一個帶有允許協定的基礎架構地址**的ACL，並允許**任何來源。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**有助於識別任何目的地為路由器的意外資料包。此ACL的最後一行必須是**permit ip any any**(IPv4)或**permit ipv6 any any**(IPv6)語句，才能允許傳輸流量。此ACL確實提供基本保護，並且允許網路工程師確保所有所需的流量都得到允許。
3. **限制源地址。**一旦您對必須允許的協定有清楚的瞭解，就可以執行進一步過濾，以僅允許這些協定的授權來源。例如，您可以明確允許外部BGP鄰居或特定GRE對等體地址。此步驟在不中斷任何服務的情況下降低了風險，並允許您對訪問基礎架構裝置的源應用精細控制。
4. **限制ACL上的目的地位址。(*可選*)**某些Internet服務提供商(ISP)可能會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可以接受協定流量的目標地址範圍。

部署示例

IPv4範例

此IPv4範例顯示根據以下定址保護路由器的基礎架構ACL:

- ISP地址塊是169.223.0.0/16。
- ISP基礎設施塊是169.223.252.0/22。
- 路由器的環回地址為169.223.253.1/32。
- 路由器是具有169.254.254.1（地址為169.223.252.1）的對等路由器和對等路由器。

顯示的基礎設施保護ACL是根據上述資訊開發的。ACL允許外部BGP對等到外部對等點、提供反欺騙過濾器以及防止基礎架構受到所有外部訪問。

```
!
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid
source addresses, and spoofs of !--- internal space (space as an external source).

!
!--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255
any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list
110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external
source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0
0.0.255.255 any !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--
- Permit only applications/protocols whose destination !--- address is part of the
infrastructure IP block. !--- The source of the traffic should be known and authorized.

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

!--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq
bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to
Protect Infrastructure

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 4 - Explicit Permit for Transit Traffic

access-list 110 permit ip any any
```

IPv6示例

此IPv6示例顯示了基於以下地址保護路由器的基礎架構ACL:

- 分配給ISP的總字首塊為2001:0DB8::/32。
- ISP用於網路基礎設施地址的IPv6字首塊為2001:0DB8:C18::/48。
- 有一台源IPv6地址為2001:0DB8:C18:2:1::1的BGP對等路由器，它與目標IPv6地址2001:0DB8:C19:2:1::F對等。

顯示的基礎設施保護ACL是根據上述資訊開發的。ACL允許外部多協定BGP對等到外部對等點，提供反欺騙過濾器，並保護基礎架構免受所有外部訪問。

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. !--- Note: This template must be
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 -
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 - Explicit Permit for
Transit Traffic permit ipv6 any any
```

相關資訊

- 存取清單支援頁面
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems