保护您的核心：基础设施保护访问控制列表

目录

简介

本文为基础设施保护访问控制列表 (ACL) 提供指南和建议部署技术。 基础设施ACL能够最小化直接基础设施攻击的风险和影响，通过只允许授权数据流传输到基础设施设备，并拒绝其他中转流量。

基础架构保护

背景

要防止路由器受到各种风险威胁（偶然和恶意威胁），基础设施保护ACL必须部署在网络入口点。这些 IPv4 和 IPv6 ACL 拒绝从外部源访问所有基础设施地址，例如路由器接口。同时，ACL允许常规传输流量流不间断，提供基本的RFC 1918、RFC 3330和反欺骗过滤。

路由器接收的数据可以分为两大类：

- 经由转发路径通过路由器的数据流
- 要通过接收路径发往路由器以供路由处理器处理的数据流

在正常运行中，大部分数据流简单地流经路由器，最后到达最后的目的地。

但是，路由处理器 (RP) 必须直接处理某些类型的数据，主要包括路由协议、远程路由器访问（如安全壳 [SSH]）和网络管理数据流（例如简单网络管理协议 (SNMP)）。 此外，诸如 Internet 控制消息协议 (ICMP) 的协议和 IP 选项可以要求直接由 RP 进行处理。通常，只有内部源中需要直接基础设施路由器访问。值得注意的几个例外包括：外部边界网关协议 (BGP) 对等体、在实际路由器上终止的协议（例如通用路由封装 [GRE] 或 IPv6 over IPv4 隧道）、用于连接测试的潜在有限 ICMP 数据包（例如响应请求或不可达 ICMP）和用于追踪路由的存活时间 (TTL) 到期消息。

注意：请记住，ICMP通常用于简单拒绝服务(DoS)攻击，并且仅在必要时允许来自外部源。

所有 RP 都有供其在其中运行的性能信封。发往 RP 的过量数据流可能会使路由器过载。导致高 CPU 使用，最终导致服务拒绝引起的数据包和路由协议丢弃。通过从外部源过滤对基础设施路由器的访问，将减少与直接路由器攻击相关的许多外部风险。来自外部源的攻击无法再访问基础设施设备。该攻击会在进入自治系统 (AS) 的输入接口上中断。

本文描述的过滤技术打算过滤指定到网络基础设施设备的数据。请勿将基础设施过滤与普通过滤混淆。基础设施保护 ACL 的唯一目的是限制协议和源可以访问关键基础设施设备的粒度级别。

网络基础设施设备包含以下区域：

- 所有路由器和交换机管理地址，包括环回接口
- 所有内部链接地址：路由器到路由器链接（点对点和多路访问）
- 不应从外部源访问的内部服务器或服务

在本文中，没有指定基础设施的所有流量，通常是指中转流量。

技术

可通过多种技术来实现基础设施保护：

- **接收 ACL (rACL)**Cisco 12000及7500支持过滤所有指定到RP的数据流的rACL，不会影响转接流量。必须明确地允许被授权的数据流，并且每个路由器必须配置rACL。请参阅 GSR：有关详细信息，请访问接收访问控制列表。
- **逐跳路由器 ACL**通过定义只允许传向路由器接口的授权流量的 ACL，拒绝转接流量以外的其他所有流量（必须明确允许），也可以保护路由器。此 ACL 在逻辑上与 rACL 类似，但不影响转接流量，因此可能对路由器的转发速率有负面影响。
- **通过基础设施 ACL 执行的边缘过滤**ACL 可以应用于网络的边缘。对于服务提供商 (SP) 而言，这是 AS 的边缘。此 ACL 可显式过滤发往基础设施地址空间的流量。边缘基础设施ACL的部署，要求您清楚地定义您的基础设施空间和访问此空间的要求/授权协议。ACL 应用到所有外部面对连接上的通往您网络的接口（例如对等体连接、客户连接等）。本文档重点讨论边缘基础设施保护 ACL 的开发和部署。

ACL 示例

以下 IPv4 和 IPv6 访问列表提供保护 ACL 所需的典型条目的简单而实际的示例。需要使用特定于本地站点的配置详细信息自定义这些基本 ACL。在双重 IPv4 和 IPv6 环境中，需要部署这两个访问列表。

IPv4 示例

```
!--- 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

必须将 IPv6 访问列表作为扩展的命名访问列表来应用。

```
!--- 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
```

注意： Log关键字可以用来提供给定协议的源和目的地的其他详细信息。虽然 **log 关键字对于 ACL 命中详细资料可提供宝贵的见解，但过多命中使用该关键字的 ACL 条目将增加 CPU 的使用率。**与日志记录相关的性能影响因平台而异。而且，使用 log 关键字将对匹配访问列表语句的数据包禁用 Cisco Express Forwarding (CEF) 交换。而是快速交换这些数据包。

开发保护 ACL

一般来说，基础设施 ACL 分为四个部分：

- 拒绝非法来源和带AS源地址的信息包从外部源进入AS的特殊使用地址和反欺骗条目**注意**：RFC 3330定义了可能需要过滤的IPv4特殊使用地址。RFC 1918 定义在 Internet 上作为无效源地址的 IPv4 保留地址空间。RFC 3513 定义了 IPv6 寻址体系结构。RFC 2827 提供入口过滤指南。
- 发往基础设施地址的明确允许的外部源流量
- **用于发往基础设施地址的所有其他外部源流量的deny 语句**
- **用于发往非基础设施目标的标准骨干流量的所有其他流量的 permit 语句**

基础设施 ACL 中的最后一行明确允许中转流量：**permit ip any any** for IPv4和**permit ipv6 any any any** for IPv6。此条目确保所有IP协议都通过核心获得允许，并且客户可以继续运行应用程序而不出现问题。

开发基础设施保护 ACL 时的第一步是了解需要的协议。虽然每个站点都有特定要求，但有些协议会经常部署，必须了解。例如，需要明确允许对外部对等体的外部 BGP。还需要明确允许需要直接访问基础设施路由器的所有其他协议。例如，如果您终止核心基础设施路由器上的GRE隧道，那么也需要明确允许协议47 (GRE)。同样，如果终止核心基础设施路由器上的 IPv6 over IPv4 隧道，那么也需要明确允许协议 41 (IPv6 over IPv4)。

可以使用分类 ACL 来帮助标识需要的协议。分类 ACL 由用于可发往基础设施路由器的各种协议的 **permit 语句组成。**有关完整列表，请参考 Cisco IOS® 软件中支持的 IP 协议上的附录。使用 **show access-list 命令显示访问控制条目 (ACE) 命中数，以标识必需的协议。**在为意外协议创建 **permit 语句之前，必须调查并了解任何可疑或意外结果。**

例如，此 IPv4 ACL 可帮助确定是否需要允许 GRE、IPSec (ESP) 和 IPv6 隧道（IP 协议 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 可用于确定是否需要允许 GRE 和 IPSec (ESP)。

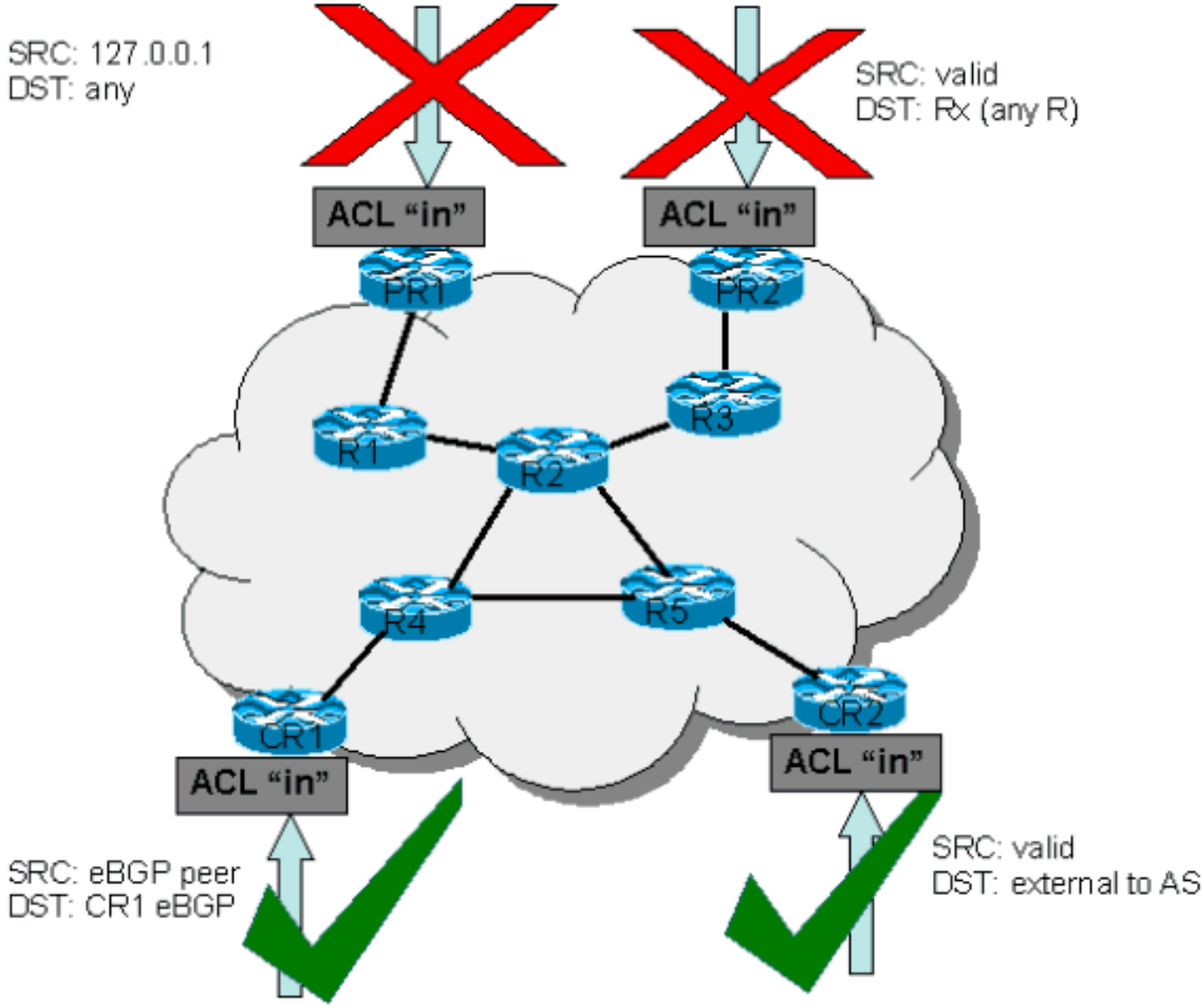
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface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

除了必需的协议外，还需要标识基础设施地址空间，因为这是 ACL 保护的空间。基础设施地址空间包括用于内部网络并很少由外部源（例如路由器接口、点到点链接寻址和重要基础设施服务）访问的任何地址。由于这些地址用于基础设施 ACL 的目标部分，因此汇总很关键。应尽可能将这些地址分组到 Classless Interdomain Routing (CIDR) 块。

使用识别的协议和地址，可以构建基础设施 ACL 以允许协议，并保护地址。除了直接保护外，ACL 还可针对 Internet 上某些类型的无效流量提供第一道重要防线。

- 必须拒绝 RFC 1918 空间。
- 必须拒绝 RFC 3330 定义的带有特殊用途地址空间的源地址的数据包。
- 必须应用反欺骗过滤器。（您的地址空间不能是来自 AS 外部的数据包的源。）

新构造的 ACL 必须在内部应用于所有入口接口。有关更多详细信息，请参阅部署指南和部署示例部分。



ACL 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。**如果没有此 **fragments 关键字，在不考虑 ACL 中的第 4 层信息时，与第 3 层语句匹配的非初始分段均受匹配条目的 permit 或 deny 语句的影响。**但是，通过添加 **fragments 关键字，可以强制 ACL 更精细地拒绝或允许非初始片段。**此行为对于 IPv4 和 IPv6 访问列表而言是相同的，不同之处在于，IPv4 ACL 允许在第 3 层和第 4 层语句中使用 fragments 关键字，IPv6 ACL 只允许在第 3 层语句内使用 fragments 关键字。

过滤片段可针对使用非初始片段（即 FO > 0）的拒绝服务 (DoS) 攻击添加额外的保护层。 在ACL的开头处使用非初始片段的Deny语句可以拒绝所有非初始片段访问路由器。在极少的情况下，有效的会话可能需要分段，而如果 ACL 中存在 **deny fragment 语句，则可能因此过滤该会话。**

例如，请考虑此部分 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>
```

将这些条目添加到 ACL 开头可拒绝任何非初始片段访问核心路由器，而非片段数据包或初始片段可

以传输到未受 **deny fragment 语句影响的 ACL 的下一行。**由于每个协议（通用数据报协议 (UDP)、TCP 和 ICMP）都会增加 ACL 中的单独计数，因此上述 ACL 命令还有助于对攻击进行分类。

这是 IPv6 的一个可比较的示例：

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

在 IPv6 ACL 开头添加此条目可拒绝任何非初始片段访问核心路由器。如上所述，IPv6 访问列表只允许在第 3 层语句内使用 fragments 关键字。

由于许多攻击依赖于向核心路由器泛洪分段数据包，因此过滤传入的分段到核心基础设施可提供额外的保护措施，并帮助确保攻击不能通过仅在基础设施ACL中匹配第3层规则来注入分段。

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

在部署基础设施保护 ACL 时，请考虑关键风险的以下两个区域：

- 确保已设置适当的 **permit**/deny 语句。对于有效的ACL，必须允许全部必需的协议，并且正确地址空间必须受到拒绝语句的保护。
- ACL 性能因平台而异。在部署 ACL 前，请查看您的硬件的性能特征。

和往常一样，我们建议您在部署之前先在实验室中对此设计进行测试。

附录

Cisco IOS 软件中支持的 IP 协议

Cisco IOS 软件支持以下 IP 协议：

- 1 – ICMP
- 2 – IGMP
- 3 – GGP
- 4 – IP in IP 封装
- 6 – TCP
- 8 – EGP
- 9 – IGRP
- 17 – UDP
- 20 – HMP
- 27 – RDP
- 41 – IPv6 in IPv4 隧道
- 46 – RSVP
- 47 – GRE
- 50 – ESP
- 51 – AH

- 53 – SWIPE
- 54 – NARP
- 55 - IP 移动
- 63 - 任何局域网
- 77 - Sun ND
- 80 – ISO IP
- 88 – EIGRP
- 89 – OSPF
- 90 – Sprite RPC
- 91 – LARP
- 94 – 与 KA9Q/NOS 兼容的 IP over IP
- 103 – PIM
- 108 – IP 压缩
- 112 – VRRP
- 113 – PGM
- 115 – L2TP
- 120 – UTI
- 132 – SCTP

部署指南

Cisco 建议您采用保守部署实践。如果要成功部署基础设施 ACL，必须熟知必需的协议，并且必须清楚地识别并定义地址空间。以下指南描述了一种使用迭代法部署保护 ACL 的保守方法。

1. **使用分类 ACL 标识网络中使用的协议。**部署一个 ACL，使其允许访问基础设施设备的所有已知协议。此发现 ACL 的源地址为 **any，目标中包括基础设施 IP 空间。**可以使用记录开发匹配协议许可语句的源地址列表。要允许流量**传输，**需要允许ip any **any(IPv4)或ipv6 any** any(IPv6)的最后一行。目的是确定特定网络使用哪些协议。应使用日志记录来进行分析，以确定还有什么可能与该路由器进行通信。**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。而且，使用 **log 关键字将对匹配访问列表语句的数据包禁用 Cisco Express Forwarding (CEF) 交换。**而是快速交换这些数据包。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. **查看已确定数据包并开始过滤对路由处理器 RP 的访问。**一旦步骤1中被ACL过滤的信息包被识别和并查看过，请用permit any source部署rACL到基础设施地址，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。使用“在末端拒绝任何…”来帮助识别指定到路由器上的所有意外的信息包。此 ACL 的最后一行必须是 **permit ip any any (IPv4) 或permit ipv6 any any (IPv6) 语句，才能允许中转流量流。**此 ACL 确实可提供基本保护，并允许网络工程师确保允许了所有必需流量。
3. **限制源地址。**一旦您清楚了解必须允许的协议，可以执行进一步过滤，只允许这些协议的核准来源。例如，您可以明确地允许外部 BGP 邻居或特定 GRE 对等地址。此步骤在不中断任何服务的情况下缩小了风险，同时允许您对访问基础设施的设备来源进行精细控制。
4. **限制ACL上的目标地址。(*可选*)**有些 Internet 服务提供商 (ISP) 可能选择只允许特定协议使用路由器中的特定目标地址。这个最终阶段用于限制可接收某个协议的数据流的目的地址范围。

部署示例

IPv4 示例

此 IPv4 示例显示基于此寻址保护路由器的基础设施 ACL：

- ISP 地址块为 169.223.0.0/16。
- ISP 基础设施块为 169.223.252.0/22。
- 路由器的环回为 169.223.253.1/32。
- 路由器是一个对等路由器，它与 169.254.254.1 对等（寻址 169.223.252.1）。

显示的基础设施保护 ACL 基于前面的信息来开发。ACL允许外部BGP等同于外部对等体，提供反欺骗过滤器，并防止基础设施受到所有外部访问。

```
!
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 示例显示基于此寻址保护路由器的基础设施 ACL：

- 已分配给 ISP 的整体前缀块为 2001:0DB8::/32。
- ISP 用于网络基础设施地址的 IPv6 前缀块为 2001:0DB8:C18::/48。
- 有一个源 IPv6 地址为 2001:0DB8:C18:2:1::1 并与目标 IPv6 地址 2001:0DB8:C19:2:1::F 对等的 BGP 对等路由器。

显示的基础设施保护 ACL 基于前面的信息来开发。ACL 允许外部多协议 BGP 与外部对等体对等，提供反欺骗过滤器，并防止对基础设施的所有外部访问。

```
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
```

相关信息

- 访问列表支持页面
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems