

中转访问控制列表：在网络边缘执行过滤

Contents

[Introduction](#)

[中转过滤器](#)

[典型设置](#)

[中转 ACL 部分](#)

[如何开发中转 ACL](#)

[标识必需协议](#)

[标识无效数据流](#)

[应用 ACL](#)

[ACL 示例](#)

[ACL 和分段数据包](#)

[风险评估](#)

[附录](#)

[常用协议和应用程序](#)

[部署指南](#)

[部署示例](#)

[Related Information](#)

[Introduction](#)

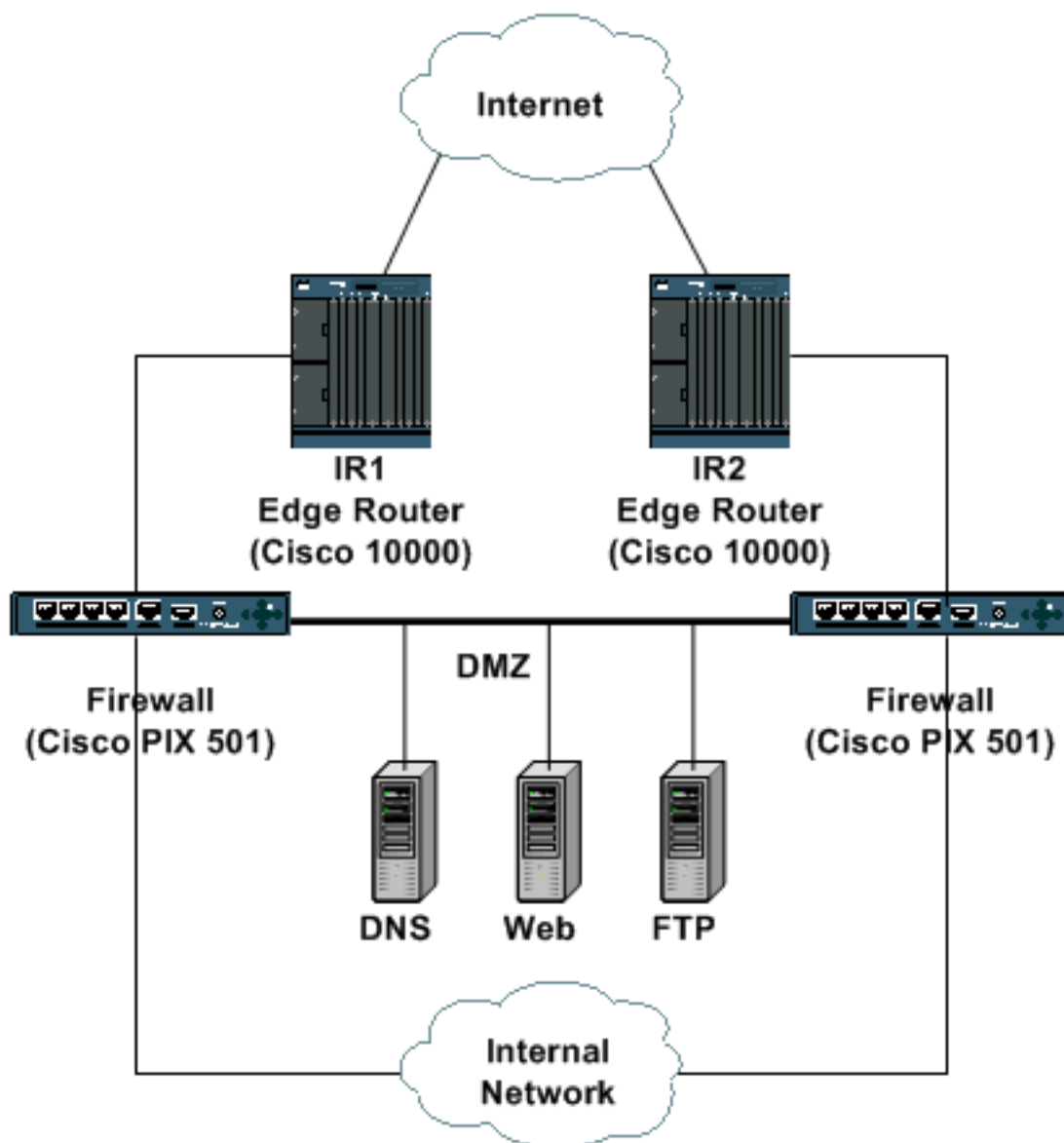
本文提供了指南和建议的配置技巧，以便在您的网络入口点过滤传输和边缘数据流。传输访问控制列表(ACL)通过明确地只允许要求的数据流通过您的网络，以增加网络的安全性。

[中转过滤器](#)

[典型设置](#)

在多数边缘网络环境里，例如典型的企业网络互联网Point of Presence，应该用于进入过滤下降未经授权流量在网络的边缘。在某些服务提供商配置，边缘或中转流量过滤的此表可能有效也用于对特定仅允许的协议限制中转流量流到/从用户。本文重点介绍企业部署模型。

此示例描述一个典型的企业 Internet 连接设计。两个边缘路由器（即 IR1 和 IR2）提供与 Internet 的直接连接。在这两路由器后，一个对防火墙(在本例中的Cisco PIXes)提供状态检测功能和存取对于内部网络和非敏感区域(DMZ)。DMZ 包含多种公用服务，如 DNS 和 Web；这是可从公用 Internet 直接访问的唯一网络。不应该直接地由互联网获取内部网络，但是从内部网络发出的数据流一定能到达互联网网站。



应该配置边界路由器通过使用Inbound ACL提供第一个安全级别。ACL允许特别地仅允许的数据流对DMZ并且允许访问互联网的内部用户的回程数据流。应在输入接口上删除所有未经授权的数据流。

中转 ACL 部分

一般说来，中转 ACL 由四个部分组成。

- 丢弃非法来源和信息包和源地址一起在您的网络内属于从进入网络从外部源的地址和special-use反电子欺骗条目Note: [RFC 1918](#) 定义 Internet 上作为无效源地址的保留地址空间。 [RFC 3330](#) 定义可能需要过滤的专用地址。 [RFC 2827](#) 提供反欺骗指南。
- 明确允许的流向 Internet 的内部连接返回数据流
- 明确允许的发往受保护的内部地址的外部源数据流
- 显式 deny 语句Note: 虽然所有 ACL 都包含隐式 deny 语句，但 Cisco 推荐使用显式 deny 语句（如 deny ip any any）。在多数平台上，这样语句维护被丢弃的信息包的数量的一计数使用 show access-list命令，可以显示。

如何开发中转 ACL

开发中转 ACL 的首要步骤是确定您的网络所需要的协议。虽然每个站点都具有特定需求，某些协议和应用程序被广泛使用，并且是最常使用的。例如，如果DMZ分段为一公共可访问的Web服务器提供连接，在端口80的DMZ服务器地址的需要从互联网的TCP。同样地，Internet 的内部连接要求 ACL 允许已建立的返回 TCP 数据流 - 即设置了确认 (ACK) 位的数据流。

标识必需协议

制定此必需协议列表可能是一项非常艰巨的任务，但可以根据需要采用多种技术来帮助标识必需数据流。

- **查看您的本地安全策略/服务策略。** 您的本地站点策略应当有助于提供所允许的服务和所拒绝的服务的基线。
- **查看/审核您的防火墙配置。** 当前防火墙配置应包含所允许的服务的显式 **permit** 语句。在许多情况下，您能转换此配置为ACL格式和使用它创建ACL条目的大多数。**Note:** 状态防火墙通常没有到授权连接的返回数据流的明确规则。由于路由器 ACL 没有状态，因此必须明确允许返回数据流。
- **查看/审核您的应用程序。** 在DMZ和那些主机的应用程序内部使用可帮助确定过滤需求。查看应用程序需求，以便提供有关过滤设计的重要详细信息。
- **使用分类 ACL。** 分类ACL由可能被注到内部网络的多种协议的许可证语句组成。（请参阅[附录 A](#) 以获取常用协议和应用程序的列表。）请使用**show access-list**命令显示一计数访问控制项 (ACE)命中识别必需的协议。在为意外协议创建显式 **permit** 语句之前，请调查并了解任何可疑或意外结果。
- **使用 NetFlow 交换功能。** Netflow 是一个交换功能，启用该功能可提供详细的流信息。如果在边缘路由器上启用了 Netflow，**show ip cache flow** 命令将提供 Netflow 记录的协议的列表。Netflow不能识别所有协议，因此必须与其他一道使用此技术。

标识无效数据流

除直接保护之外，传输ACL在互联网应该也提供第一个防御范围对无效的数据流特定类型的。

- 拒绝 RFC 1918 空间。
- 丢弃信息包和属于special-use地址空间的源地址一起，如对RFC 3330定义。
- 根据 RFC 2827 应用反欺骗过滤器；您的地址空间不应该是信息包的来源从您的自治系统 (AS)之外。

要考虑的其他数据流类型包括：

- **需要与边缘路由器通信的外部协议和 IP 地址服务提供商 IP 地址的 ICMP路由协议IPSec VPN (如果将边缘路由器用作终端)**
- **明确允许的流向 Internet 的内部连接返回数据流特定互联网控制消息协议(ICMP)类型 outbound域名系统(DNS)查询回复已建立的 TCP用户数据报协议(UDP)回程数据流FTP数据连接TFTP 数据连接多媒体连接**
- **明确允许的发往受保护的内部地址的外部源数据流VPN 数据流Internet 安全关联和密钥管理协议 (ISAKMP)网络地址转换(NAT)穿越专用封装封装安全有效载荷(ESP)认证报头(AH)Web 服务器的 HTTP对Web服务器的安全套接字层SSLFTP 服务器的 FTP入站 FTP 数据连接入站 FTP 被动 (pasv) 数据连接简单邮件传输协议(SMTP)其他应用程序和服务器入站 DNS 查询入站 DNS 区域传输**

应用 ACL

最近被修建的ACL应该是应用入站在边界路由器的面向互联网的接口。在[典型设置](#)部分演示的示例中，在 IR1 和 IR2 面向 Internet 的接口上应用了 ACL。

有关详细信息，请参阅[部署指南](#)和[部署示例](#)部分。

ACL 示例

此访问列表提供中转 ACL 所需的典型条目的示例，此示例非常简单，但却切实可行。需要使用特定于本地站点的配置详细信息自定义此基本 ACL。

```
!--- Add anti-spoofing entries. !--- Deny special-use address sources. !--- Refer to RFC 3330
for additional special use addresses.
```

```
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
access-list 110 deny ip host 255.255.255.255 any
```

```
!--- The deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.
```

```
access-list 110 deny ip host 0.0.0.0 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 !---
Permit Border Gateway Protocol (BGP) to the edge router. access-list 110 permit tcp host
bgp_peer gt 1023 host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host
router_ip gt 1023 !--- Deny your space as source (as noted in RFC 2827). access-list 110 deny ip
your Internet-routable subnet any !--- Explicitly permit return traffic. !--- Allow specific
ICMP types.
```

```
access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq 53 host primary DNS
server gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-list 110
permit udp any eq 53 host primary DNS server eq 53 !--- Permit legitimate business traffic.
access-list 110 permit tcp any Internet-routable subnet established access-list 110 permit udp
any range 1 1023 Internet-routable subnet gt 1023 !--- Allow ftp data connections. access-list
110 permit tcp any eq 20 Internet-routable subnet gt 1023 !--- Allow tftp data and multimedia
connections. access-list 110 permit udp any gt 1023 Internet-routable subnet gt 1023 !---
Explicitly permit externally sourced traffic. !--- These are incoming DNS queries.
```

```
access-list 110 permit udp any gt 1023 host <primary DNS server> eq 53
!-- These are zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
secondary DNS server gt 1023 host primary DNS server eq 53 !--- Permit older DNS zone transfers.
access-list 110 permit tcp host secondary DNS server eq 53 host primary DNS server eq 53 !---
Deny all other DNS traffic. access-list 110 deny udp any any eq 53 access-list 110 deny tcp any
any eq 53 !--- Allow IPSec VPN traffic. access-list 110 permit udp any host IPSec headend device
eq 500 access-list 110 permit udp any host IPSec headend device eq 4500 access-list 110 permit
50 any host IPSec headend device access-list 110 permit 51 any host IPSec headend device access-
list 110 deny ip any host IPSec headend device !--- These are Internet-sourced connections to !-
-- publicly accessible servers. access-list 110 permit tcp any host public web server eq 80
access-list 110 permit tcp any host public web server eq 443 access-list 110 permit tcp any host
public FTP server eq 21 !--- Data connections to the FTP server are allowed !--- by the permit
established ACE. !--- Allow PASV data connections to the FTP server.
```

```
access-list 110 permit tcp any gt 1023 host public FTP server gt 1023 access-list 110 permit tcp
any host public SMTP server eq 25 !--- Explicitly deny all other traffic.
```

```
access-list 101 deny ip any any
```

Note: 当应用中转 ACL 时，请牢记这些建议。

- **log** 关键字可用于提供有关给定协议的源和目标的其他详细信息。虽然使用日志关键字增量 CPU 利用率的此关键字提供重要的见解到 ACL 命中详细资料，对 ACL 条目的额外的命中。与日志记录相关的性能影响因平台而异。
- 对于因管理原因而被 ACL 拒绝的数据包，将生成 ICMP 不可达消息。这可能会影响路由器和链路性能。请考虑使用 **no ip unreachable** 命令，以便在部署有中转（边缘）ACL 的接口上禁用 IP 不可达功能。
- 开始时可以使用所有 **permit** 语句部署此 ACL，以便确保不会拒绝企业合法数据流。一旦企业合法数据流被识别并且占了，特定**拒绝**元素可以被配置。

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。通常情况下，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（协议、源地址和目标地址）均受匹配条目的 **permit** 或 **deny** 语句的影响。注意使用片段关键字能强制 ACL 对拒绝或允许与更多粒度的非初始片段。

过滤片段添加一个另外的层防护使用仅非初始片段的拒绝服务攻击(例如 FO > 0)。在 ACL 的开头处针对非初始分段使用 **deny** 语句可以拒绝所有非初始分段访问路由器。在少见情况下，如果**拒绝片段**语句存在于 ACL，有效的会话也许要求分段并且被过滤。可能导致分段的情况包括使用数字证书进行 ISAKMP 身份验证和使用 IPsec NAT Traversal。

例如，请考虑此处显示的部分 ACL。

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

而不分段的信息包或初始分段通过对未受影响的 ACL 的下条线路**拒绝片段**语句，添加这些条目到 ACL 的初期拒绝对网络的所有非初始片段访问。由于每个协议（UDP、TCP 和 ICMP）都会增加 ACL 上的单独计数，上述 ACL 代码片断还能有助于对攻击进行分类。

因为许多攻击依靠与分段的信息包的泛滥，对内部网络的过滤流入片段提供保护一个被添加的方案，并且帮助保证攻击不能通过匹配在传输 ACL 的第 3 层规则注入片段。

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

当部署中转数据流保护 ACL 时，请考虑两个主要风险领域。

- 确保已设置适当的 **permit/deny** 语句。为使 ACL 行之有效，必须允许全部必需协议。
- 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。

Cisco 建议您在部署前先在实验室测试该设计。

附录

常用协议和应用程序

TCP 端口名称

当您配置在Cisco IOS软件时的ACL TCP端口名字此列表可以使用而不是端口号。请参阅最新指定编号的 RFC，以便查找这些协议的相关参考资料。当配置 ACL 时，您也可以通过输入？(而不是端口号) 找到与这些协议对应的端口号。

| | |
|----------|------------|
| bgp | kshell |
| chargen | 登录 |
| cmd | lpd |
| 白天 | nntp |
| 丢弃 | pim |
| 域 | pop2 |
| 响应 | pop3 |
| exec | smtp |
| finger | sunrpc |
| ftp | Syslog |
| ftp-data | tacacstalk |
| Gopher | telnet |
| 主机名- | 时间 |
| ident | uucp |
| irc | 域名查询程序 |
| klogin | www |

UDP 端口名称

当在 Cisco IOS 软件中配置 ACL 时，可以使用此 UDP 端口名称列表，而不使用端口号。请参阅最新指定编号的 RFC，以便查找这些协议的相关参考资料。当配置 ACL 时，您也可以通过输入？(而不是端口号) 找到与这些协议对应的端口号。

| | |
|-------------|-------------|
| 一击 | ntp |
| bootpc | pim-auto-rp |
| bootps | RIP |
| 丢弃 | snmp |
| dnsix | snmptrap |
| 域 | sunrpc |
| 响应 | Syslog |
| isakmp | TACACS |
| mobile-ip | 谈话 |
| 名称服务程序 | tftp |
| netbios-dgm | 时间 |

| | |
|------------|-------|
| netbios-ns | 谁 |
| netbios-ss | xdmcp |

部署指南

Cisco 建议您采用保守部署实践。您必须对所需协议具有清楚的认识，才能成功部署中转 ACL。这些指南介绍了一种非常保守的方法，来部署采用迭代方法的保护 ACL。

1. **使用分类 ACL 标识网络中使用的协议。**配置允许所有已知协议在网络使用的ACL。此发现（或分类）ACL 应具有任何源地址和一个 IP 地址/可通过 Internet 路由的整个 IP 子网的目标。配置允许 **ip any any log** 的最后一个条目，以便帮助标识您需要允许的其他协议。其目标在于：确定网络上正在使用的所有必需协议。使用日志记录进行分析，确定可能与路由器通信的其他内容。**Note:** 虽然日志关键字提供重要的见解到ACL命中详细资料，对ACL条目的额外的命中使用的此关键字也许导致巨大数字日志条目和可能高路由器CPU使用方法。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。请注意，如果设置的 ACL 包含所有 **permit** 语句，网络将面临攻击风险。尽快执行分类进程，以便适当的访问控制可以被进行。
2. **查看已标识的数据包，并开始过滤对内部网络的访问。**一旦识别并且查看了step1的ACL过滤的信息包，请更新分类ACL占新识别协议和IP地址。添加用于反欺骗的 ACL 条目。如果需要，请在分类 ACL 中用特定 **deny** 条目替换 **permit** 语句。您能使用**show access-list**命令监控特定**拒绝**条目可以为命中计数被监控。这会提供有关禁止的网络访问尝试的信息，而不必对 ACL 条目启用日志记录。ACL 的最后一行应为 **deny ip any any**。再次，最后条目的命中计数能提供关于禁止的访问企图的信息。
3. **监控并更新 ACL。**监控完整的 ACL，确保控制添加新引入的必需协议。监控 ACL 时，还会提供有关禁止的网络访问尝试的信息，这些尝试可提供迫在眉睫的攻击的相关信息。

部署示例

此示例演示可根据以下地址保护网络的中转 ACL。

- ISP 路由器的 IP 地址是 10.1.1.1。边缘路由器面向 Internet 的 IP 地址是 10.1.1.2。可通过 Internet 路由的子网是 192.168.201.0 255.255.255.0。VPN 前端是 192.168.201.100。Web 服务器是 192.168.201.101。FTP 服务器为 192.168.201.102。SMTP 服务器为 192.168.201.103。主要 DNS 服务器是 192.168.201.104。辅助 DNS 服务器是 172.16.201.50。

中转保护 ACL 根据此信息开发。ACL允许eBGP对等体到ISP路由器，提供反欺骗过滤器，允许特定回程数据流，允许特定Inbound数据流和明确地否决其他数据流。

```
no access-list 110
!--- Phase 1 - Add anti-spoofing entries. !--- Deny special-use address sources. !--- See RFC
3330 for additional special-use addresses.

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
access-list 110 deny ip host 255.255.255.255 any
!--- This deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny ip host 0.0.0.0 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 !---  
Permit BGP to the edge router. access-list 110 permit tcp host 10.1.1.1 gt 1023 host 10.1.1.2 eq  
bgp access-list 110 permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1023 !--- Deny your space  
as source (as noted in RFC 2827). access-list 110 deny ip 192.168.201.0 0.0.0.255 any !--- Phase  
2 - Explicitly permit return traffic. !--- Allow specific ICMP types.
```

```
access-list 110 permit icmp any any echo-reply  
access-list 110 permit icmp any any unreachable  
access-list 110 permit icmp any any time-exceeded  
access-list 110 deny icmp any any  
!--- These are outgoing DNS queries. access-list 110 permit udp any eq domain host  
192.168.201.104 gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-  
list 110 permit udp any eq domain host 192.168.201.104 eq domain !--- Permit legitimate business  
traffic. access-list 110 permit tcp any 192.168.201.0 0.0.0.255 established access-list 110  
permit udp any range 1 1023 192.168.201.0 0.0.0.255 gt 1023 !--- Allow FTP data connections.  
access-list 110 permit tcp any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023 !--- Allow TFTP data  
and multimedia connections. access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt  
1023 !--- Phase 3 - Explicitly permit externally sourced traffic. !--- These are incoming DNS  
queries.
```

```
access-list 110 permit udp any gt 1023 host 192.168.201.104 eq domain  
!--- Zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host  
172.16.201.50 gt 1023 host 192.168.201.104 eq domain !--- Permit older DNS zone transfers.  
access-list 110 permit tcp host 172.16.201.50 eq domain host 192.168.201.104 eq domain !--- Deny  
all other DNS traffic. access-list 110 deny udp any any eq domain access-list 110 deny tcp any  
any eq domain !--- Allow IPsec VPN traffic. access-list 110 permit udp any host 192.168.201.100  
eq isakmp access-list 110 permit udp any host 192.168.201.100 eq non500-isakmp access-list 110  
permit esp any host 192.168.201.100 access-list 110 permit ahp any host 192.168.201.100 access-  
list 110 deny ip any host 192.168.201.100 !--- These are Internet-sourced connections to !---  
publicly accessible servers. access-list 110 permit tcp any host 192.168.201.101 eq www access-  
list 110 permit tcp any host 192.168.201.101 eq 443 access-list 110 permit tcp any host  
192.168.201.102 eq ftp !--- Data connections to the FTP server are allowed !--- by the permit  
established ACE in Phase 3. !--- Allow PASV data connections to the FTP server.
```

```
access-list 110 permit tcp any gt 1023 host 192.168.201.102 gt 1023  
access-list 110 permit tcp any host 192.168.201.103 eq smtp
```

!--- **Phase 4 - Add explicit deny statement.**

```
access-list 110 deny ip any any
```

```
Edge-router(config)#interface serial 2/0  
Edge-router(config-if)#ip access-group 110 in
```

[Related Information](#)

- [访问列表支持页面](#)
- [Cisco IOS 交换服务命令参考, 版本 12.2 - 命令 : access-list rate-limit through ip cef](#)
- [请求注解 \(RFC\)](#)
- [Technical Support & Documentation - Cisco Systems](#)