

8 防火墙安全策略及其配置

2019年5月27日 10:02

1 防火墙如何开发安全策略

- [1.1 什么是安全策略](#)
- [1.2 安全策略的重要性](#)
- [1.3 确定有效的安全策略所需要达到的目标](#)
- [1.4 构建安全策略的7步](#)
- [1.5 考虑防火墙的不足](#)
- [1.6 其他的安全策略主题](#)
- [1.7 定义针对违反安全规则的响应](#)
- [1.8 客服管理的障碍](#)

2 防火墙配置概述

3 Cisco IOS 防火墙特征集

4 配置Cisco IOS 防火墙包过滤功能

- [4.1 配置访问控制列表](#)
- [4.2 翻转掩码](#)
- [4.3 配置标准访问控制列表](#)
- [4.4 配置扩展访问控制列表](#)
- [4.5 配置标识访问控制列表](#)
- [4.6 配置动态访问控制列表](#)
- [4.7 访问控制列表配置要点](#)

1 防火墙如何开发安全策略

- [1.1 什么是安全策略](#)
- [1.2 安全策略的重要性](#)
- [1.3 确定有效的安全策略所需要达到的目标](#)
- [1.4 构建安全策略的7步](#)
- [1.5 考虑防火墙的不足](#)
- [1.6 其他的安全策略主题](#)
- [1.7 定义针对违反安全规则的响应](#)
- [1.8 客服管理的障碍](#)

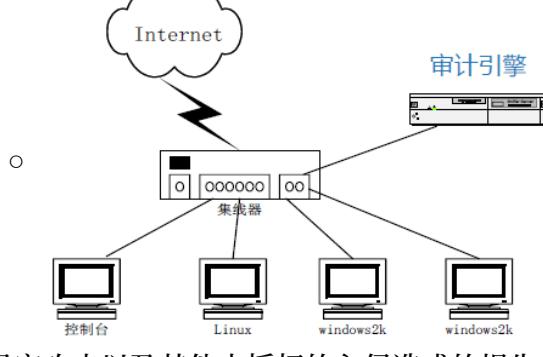
1.1 什么是安全策略

- 一个有效的防火墙依赖于一个明确清楚的、全面的安全策略。实际上，在设计安全系统时首先考虑的应该是策略，而不是防火墙。
- 定义：一个列出必须满足的特定需求或规则的文档
- 与策略相关名词：
 - 标准：所有用户都必须满足的系统提出的特殊需求的集合
 - 方针：一些好的实践建议

1.2 安全策略的重要性

- 防火墙的设计依赖于被保护资源和那些资源所面临的危险，两者都包括在安全策略中。
- 策略还告诉建立什么类型的入侵检测和审计系统
- 审计是指由专门的机构和人员，以国家法律法规为依据，对国家政府机关、企事业单位的财政、财务收支及有关经济活动的真实性、合法性、效益性进行审查，评价经济责任，用以维护财经法纪，改善经营管理，提高经济效益，促进宏观调控的独立性的经济监督活动。
- 近年来，随着信息技术的不断发展，信息系统日渐成为现代社会中不可缺少的"基础设施"。
- 就在信息系统为人们提供便利，满足社会服务需求的同时，信息系统自身的结构、功能复杂度越来越高，使得信息系统本身由于复杂度增大导致的系统脆弱性隐患变得越发严重。

- 对信息系统进行错误操作、滥用、不正当使用导致的社会问题屡见不鲜，给社会带来了巨大的经济损失。
- 近年来网络化趋势使得这种影响波及范围更为扩大，造成了极为恶劣的影响。因此，信息系统的安全性愈来愈为社会所关注。
- 任何技术都是“双刃剑”，信息系统给社会带来巨大便利的同时，也往往会被“不法分子”所利用。如何杜绝这类现象，如何防止信息系统因为自身的缺陷给社会蒙受巨大损失，这又是面临的另一个新课题。
- 如何对待信息系统投资也引起人们的逐步关注。不少信息系统建设项目劳民伤财，耗资巨大却无法为社会提供实际的服务价值，甚至还危害及社会。对于企业来说是一笔重大的经济损失。
- 应对信息系统的建设，需要引入一种新的管理机制来对信息系统的安全性、投资效果、实施进程和实施效果等进行评估、指导和改进。这种机制就是IT审计。
- 为什么要进行网络审计？
 - 我们的网络中到底发生了什么
 - 如何进行事后的追踪
 - 如何对网络进行有效的监控
 - 如何改进网络的安全策略
- 网络审计的主要内容：
 - 网络连接审计
 - 协议审计
 - 端口审计
 - 拨号连接审计
 - 个人帐户审计
 - 文件访问审计
 - 数据审计
 - 流量统计审计
 - 数据库审计
 - WEB服务器审计
 - 安全事件再现审计
 - 键盘审计
 - 屏幕审计
 - 系统统计分析
- 审计产品部署



- 黑客攻击以及其他未授权的入侵造成的损失：
 - 雇员时间
 - 数据丢失
 - 生产力

1.3 确定有效的安全策略所需要达到的目标

- 要清楚地描述一个安全的网络计算环境
- 要灵活适应公司结构的任何改动
- 要保证在整个公司中一致地交流和执行
- 要明确雇员对网络的使用权限
- 要对雇员和管理人员关于隐私和安全的合理和不合理的表现进行明确定义

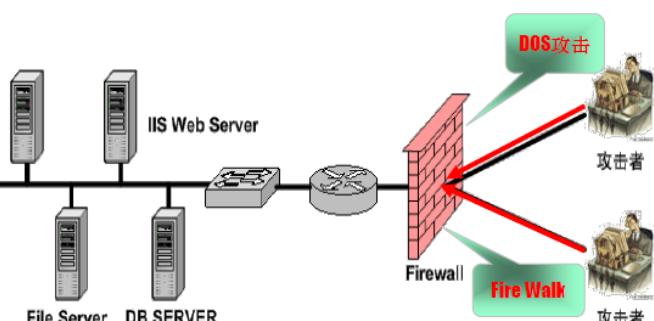
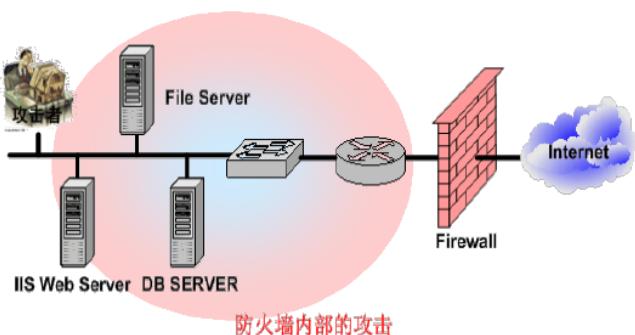
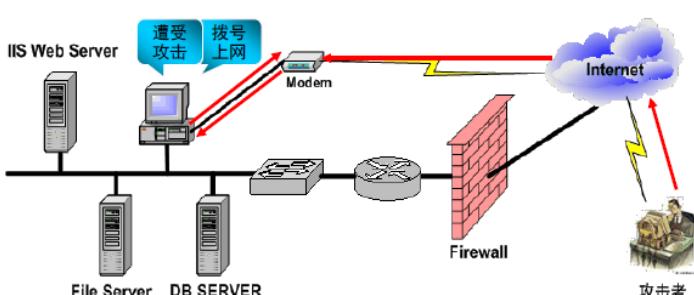
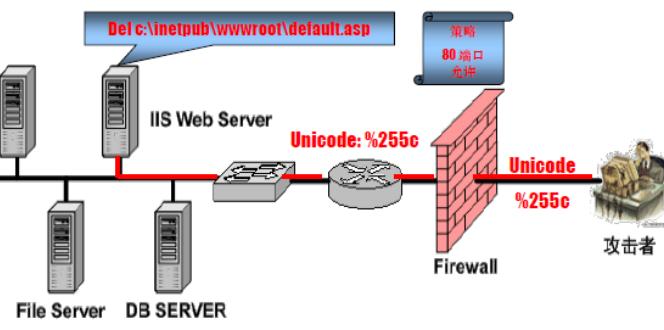
1.4 构建安全策略的7步

- 组件一个团队
- 制定公司的整体安全策略
- 确定被保护的资产

- 决定安全策略审核的内容
- 确定安全风险
- 定义可接受的使用策略
- 提供远程访问

1.5 考虑防火墙的不足

- 超出防火墙所能处理的过多的网络访问量，及其防火墙崩溃的蛮力攻击
- 在网络中将一个加密的带有病毒的电子邮件消息发送给某人，加密的消息将会通过防火墙，这样病毒就会传染给系统
- 若雇员将远程访问号码泄漏，则未经授权的用户就能够访问公司网络
- 雇员将密码泄露
- 防火墙属于静态防护
- 防火墙难于防内
- 防火墙难于管理和配置，易造成安全漏洞
- 防火墙的安全控制主要是基于IP地址的，难于为用户在防火墙内提供一致的安全策略
- 防火墙只实现了粗粒度的访问控制，且不能与企业内部使用的其它安全机制（如访问控制）集成使用
- 任何一个系统（尤其是底层系统和应用系统）中可能存在着安全漏洞，造成绕过防火墙的攻击



1.6 其他的安全策略主题

- 密码—加密
- 限制可移动介质
- ASP
- 可接受的用户
- 笔记本电脑安全使用
- 无线安全
- VPN的使用

1.7 定义针对违反安全规则的响应

- 记录数据
- 响应处理联系人
- 响应策略

1.8 客服管理的障碍

- 雇员的培训
- 呈交并回顾制定过程
- 改进安全策略

2 防火墙配置概述

- 非法数据包渗透一个应用得当、配置完善的防火墙是十分困难的。
- 在实际应用中人们一方面对网络安全的意识十分薄弱，另一方面在网络安全产品尤其防火墙的配置策略中漏洞百出，因此给网络攻击者可乘之机。

3 Cisco IOS防火墙特征集

- 基于Cisco IOS的防火墙特性集 (FFS, FirewallFeaturesSet)，能够实现对Cisco 路由器提供附加的安全功能，方便地实现边界安全部署。
- IOSFFS的优势在其子接口类型、端口密度、性能以及形态元素（即大小、形式和容量）方面巨大的灵活性。
- CiscoIOSFFS的核心是基本防火墙工具——基于上下文的访问控制(Context-basedAccessControl, CBCA)。
- CBCA是一种状态检查防火墙，作为路由器的操作系统IOS的附加特性集运行。
- CBCA实现了防火墙的一些重要功能和服务。

4 配置Cisco IOS防火墙包过滤功能

- 在Cisco IOS防火墙特征集中集成了很强的防火墙功能和入侵检测功能。
- Cisco IOS防火墙包过滤技术依赖于访问控制列表 (ACL, AccessControlList)。
- 根据对数据包检查的粒度，Cisco IOS防火墙将访问控制列表分为两类：标准访问控制列表和扩展访问控制列表。
- 根据功能和特点，访问控制列表还可以分为：静态访问控制列表、动态访问控制列表和反射访问控制列表。
- 字符串匹配
- 匹配串：BBCABCDABCABCABCDABCABDE
- 模式串：ABCDABD
- 匹配算法：
 - BruteForce(BF或蛮力搜索)算法
 - KMP算法
 - Horspool算法
- [4.1 配置访问控制列表](#)
- [4.2 翻转掩码](#)
- [4.3 配置标准访问控制列表](#)
- [4.4 配置扩展访问控制列表](#)
- [4.5 配置标识访问控制列表](#)
- [4.6 配置动态访问控制列表](#)
- [4.7 访问控制列表配置要点](#)

4.1 配置访问控制列表

- Cisco IOS访问控制列表的配置需要遵循两个步骤：

- 创建访问控制列表
- 将访问控制列表绑定到某个网络接口
- 配置访问控制列表的时候，需要为每一个访问控制列表分配一个惟一的数字以标识这个列表，Cisco公司对基于IOS的各种访问控制列表的编号进行了限制和定义，见下表

- 配置访问控制列表

Cisco IOS访问控制列表编号列表

IP访问控制列表	编号范围
标准访问控制列表	1-99
扩展访问控制列表	100-199
IPX访问控制列表	编号范围
标准访问控制列表	800-899
扩展访问控制列表	900-999
SAP*访问控制列表	1000-1099

*SAP, Service Advertising Protocol, 服务广告协议。

- 配置访问控制列表——创建访问控制列表

- 创建访问控制列表就是向某个访问控制列表中添加命令的过程。命令的一般格式是：命令+访问控制列表编号+操作+条件

- 创建某个访问控制列表并添加一条命令语句
 - Router(config)#access-list access-list-number[permit|deny]测试条件
 - 删除某个访问控制列表
 - Router(config)#noaccess-list access-list-number

- 说明：

- 可以向同一个访问控制列表写入多条语句；
- 访问控制列表的配置命令比较繁琐，可以使用文本文件事先将命令编辑好，再复制粘贴至IOS中；
- 使用“noaccess-list access-list-number”命令将删除整个访问控制列表。在标准和扩展访问控制列表中，不能删除访问控制列表中的某一条命令语句，只能一次删除整个访问控制列表。

- 配置访问控制列表——绑定访问控制列表到网络接口

- 创建访问控制列表后必须将其绑定到Cisco IOS防火墙或路由器的某个接口方能生效。

- 绑定访问控制列表到某网络端口命令

- Router(config-if)#protocol access-group access-list-number[in|out]
 - 参数 protocol 指明了是针对哪种协议的访问控制列表。常用的有 IP、IPX 等。参数 in/out 表明数据流进入／流出网络接口的方向。

4.2 翻转掩码 (wildcard bits)

- 在Cisco ISO中，网络地址的辨别和匹配不是通过子网掩码，而是通过翻转掩码。与子网掩码类似，翻转掩码是由0和1组成的32位二进制数字，分成4段。32位中的每一位正好可以和二进制IP地址的相应位对应。

十进制网络地址	192.168.9.1/255.255.255.0			
二进制IP地址	11000000	10100100	00001001	00000001
二进制子网掩码	11111111	11111111	11111111	00000000
二进制翻转掩码	00000000	00000000	00000000	11111111

4.3 配置标准访问控制列表

- 标准访问控制列表用于允许或者禁止来自于某个网络的所有数据流，或者禁止某一协议的数据流。标准访问控制列表配置命令有：

- Router(config)#access-list access-list-number[permit|deny] source-ip wildmask
 - 创建标准访问控制列表。访问控制列表编号范围必须是1-99。默认翻转掩码是0000。
- Router(config-if)#ip access-group access-list-number[in|out]
 - 将一个已存在的访问控制列表绑定到某个接口上。参数 In|out 指明是入栈访问控制列表还是出栈访问控制列表，默认为出栈访问控制列表。
- Router#show access-list[access-list-number]

- 查看已经存在的访问控制列表包含的命令语句，如果不指定ACL编号，则显示所有的访问控制列表。
- Router#showipinterface interface
 - 查看是否为某个接口绑定了访问控制列表。
 - 注意：每一个网络接口在每个数据流方向上针对每一个协议只允许存在一个访问控制列表。配置实例：
 - Router(config)#access-list1 permit 1915340000255
 - Router(config)#access-list1 permit 128880000255255
 - Router(config)#access-list1 permit 360000255255255
 - 使用检测命令，可以得到相关配置的调试信息：
 - Router(config)#showaccess-list1
- 配置标准访问控制列表——例1指定特定网络
 - 任务：如下图所示，在防火墙/路由器上，只允许来自于网络172.16.0.0的数据包被转发出去，其余的数据包都将被阻止。
- 第一步，创建标准访问控制列表，命令如下：
 - Router(config)#access-list1 permit 172160000255255
- 第二步，将访问控制列表绑定到E0和E1的出口上，命令如下：
 - Router(config)#interface E0
 - Router(config-if)#ipaccess-group1out
 - Router(config)#interface E1
 - Router(config-if)#ipaccess-group1out
- 配置标准访问控制列表——例2阻止特定地址
 - 任务：在防火墙/路由器上，在接口E0阻止来自特定地址172.16.4.13的数据流，其他的数据流将被转发出去。
 - 第一步，创建标准访问控制列表，命令如下：
 - Router(config)#access-list1 deny 172164130000
 - Router(config)#access-list1 permit any
 - 第二步，绑定，命令如下：
 - Router(config)#interface E0
 - Router(config-if)#ipaccess-group1out
 - 说明：第一个access-list命令用“deny”参数来禁止来自于这个指定主机的数据流，地址掩码0000表明要检查、匹配地址中的所有的位。第二个access-list命令中，any代表“0000255255255”，表示允许源自任何网络的数据流通过。
- 配置标准访问控制列表——例3阻止特定的子网
 - 任务：阻止来自于特定子网172.16.4.0的数据通过E0端口，而转发其他的数据。
 - 第一步，创建标准访问控制列表，命令如下：
 - Router(config)#access-list1 deny 1721640000255
 - Router(config)#access-list1 permit any
 - 第二步，绑定，命令如下：
 - Router(config)#interface E0
 - Router(config-if)#ipaccess-group1out

4.4 配置扩展访问控制列表

- 扩展访问控制列表对数据包的控制比标准访问控制列表粒度更细，因而运用更广。
 - 例如，可以使用扩展访问控制列表来实现允许web数据流，而禁止FTP或Telnet数据流。
 - 扩展访问控制列表可以检查源地址和目标地址、特定的协议、端口号，以及其他参数。
 - 这些特性使得扩展访问控制列表可以更加灵活地描述数据过滤任务
 - 在Cisco IOS中，扩展访问控制列表使用的编号数字范围是：100-199。
- 扩展访问控制列表配置命令：
 - 创建一个扩展访问控制列表

- Router(config)#access-list access-list-number [permit | deny]
 - protocol source source-mask [operator port] destination destination-mask [operator port]
- 参数说明:
 - access-list-number: 范围100-199。用于标识访问控制列表;
 - protocol: 可以是IP, TCP, UDP, ICMP, GRE, IGRP, 指明源数据包的协议类型;
 - source/destination-mask: 源地址、源掩码;
 - operator/port: TCP协议端口号范围, 可以是lt (小于)、gt (大于)、eq (等于)、neq (不等于) 某个端口号;
 - destination/destination-mask: 目的地地址、目的掩码。

○ 绑定访问控制列表到某个网络接口上

- Router(config-if)#ip access-group access-list-number [in|out]

○ 显示访问控制列表包含的命令语句

- Router#show access-list [access-list-number]

○ 查看是否为某个接口绑定了访问控制列表

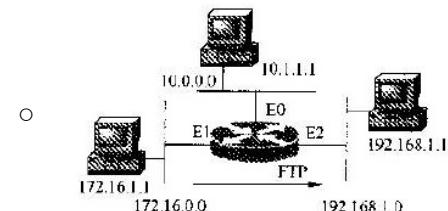
- Router#show ip interface interface:

○ 在扩展访问控制列表配置中经常通过一些端口号控制一些应用层服务数据包, 下边的表列出了一些常见的应用层服务和TCP/UDP端口号的对应关系。

常见的端口号	IP协议
20	FTP, 数据
21	FTP, 控制
○ 23	Telnet
25	SMTP
53	DNS
80	HTTP

· 例4使用扩展访问控制列表

○ 任务: 如图所示, 在防火墙/路由器上, 要求只有主机172.16.1.1能够通过FTP访问网络192.168.1.0。



○ 第一步, 创建扩展的访问控制列表, 命令如下

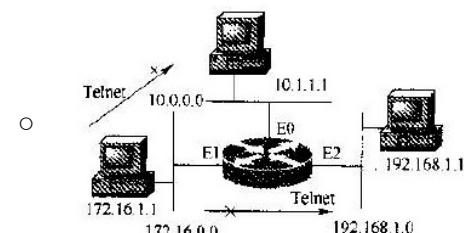
- Router(config)#access-list 100 permit TCP 172.16.1.1 0.0.0.0 eq 20
- 192.168.1.0 0.0.0.255 eq 20

○ 第二步, 将访问控制列表绑定到E2的出口:

- Router(config)#interface E2
- Router(config-if)#ip access-group 100 out

· 例5使用扩展访问控制列表

○ 任务: 拒绝网络172.16.0.0通过Telnet访问任何网段, 允许其他所有的IP数据。



○ 第一步, 创建扩展的访问控制列表, 命令如下

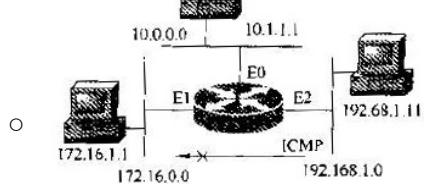
- Router(config)#access-list 101 deny TCP 172.16.0.0 0.0.0.255 any eq 23
- Router(config)#access-list 101 permit ip any any

○ 第二步, 将访问控制列表绑定到E1的入口:

- Router(config)#interface E1
- Router(config-if)#ip access-group 101 in

· 例6使用扩展访问控制列表

○ 任务: 禁止网络192.168.1.0使用ping命令访问网络172.16.0.0, 允许其他的IP数据。



- 第一步，创建扩展访问控制列表，命令如下：
 - Router(config)#access-list 199 deny icmp 192.168.1.0 0.0.0.255 172.16.0.0 0.0.0.255 255 255
 - Router(config)#access-list 199 permit ip any any
- 第二步，将访问控制列表绑定到E2的入口：
 - Router(config)#interface E2
 - Router(config-if)#ip access-group 199 in
- 在路由器上，对于给定的协议，当需要的配置超出了99个标准访问控制列表或100个扩展访问控制列表时可以采用命名访问控制列表。即使用字符串代替数字来标识访问控制列表，称为命名（Named）访问控制列表。

4.5 配置标识访问控制列表

- 命名访问控制列表作为一种特殊的访问控制列表，具有优点如下：
 - 可以用有含义的字符串直观标识一个访问控制列表
 - 当修改访问控制列表中的某一条语句时，可以在不删除整个访问控制列表的情况下修改它
- 使用命名访问控制列表的注意事项：
 - 命名访问控制列表与Cisco IOS 12之前的版本不兼容
 - 命名访问控制列表可包含标准和扩展访问控制列表
 - 不能为多个访问控制列表使用相同的名字
- 命名访问控制列表配置命令
 - 创建一个命名访问控制列表
 - Router(config)#ip access-list [standard|extended] name
 - standard和extended指明是标准还是扩展的访问控制列表，参数name是标识访问控制列表的名称的字符串。命令执行后进入如下模式：
 - Router(config[std|ext-nacl])#
 - 向命名访问控制列表中写入命令语句
 - Router(config[std|ext-nacl])#[permit|deny] test condition
 - 删除命名访问控制列表中的某一条语句
 - Router(config[std|ext-nacl])#no[permit|deny] test condition
 - 注意：该访问控制列表仍然存在，这与用数字标识的访问控制列表不同。
 - 绑定命名访问控制列表
 - Router(config-if)#ip access-group name [in|out]

4.6 配置动态访问控制列表

- 配置动态访问控制列表可以实现访问控制列表的动态改变。动态访问控制列表（也叫Lock and Key）是在Cisco IOS Release 11.1引入的。这个特性是依靠于telnet，验证（authentication，本地和远程）还有扩展ACL。当验证通过以后，才允许telnet。
- 动态访问控制列表配置命令如下：
 - 配置动态访问控制列表，作为临时访问控制列表条目的模板和占位符


```
access-list access-list-number [dynamic dynamic-name]
[timeout minutes] {permit | deny} telnet source source-
• wildcard destination destination-wildcard [precedence
precedence] [tos tos] [established] [log]
```
 - 配置接口
 - interface type number
 - 在接口配置模式下，将访问控制列表用于接口
 - ip access-group access-list-number [in|out]
 - 在全局模式下，定义一个或多个虚拟终端（VTY）端口
 - line VTY line-number [ending-line-number]
 - 如果指定多个VTY端口，则它们的配置必须相同，因为软件循环地搜索可用的VTY端口。

○ 配置用户身份验证

```
username name password secret
```

- login trcacs

```
password password login local
```

○ 启用创建临时访问列表条目功能

- autocommandaccess-enable[host][timeoutminutes]

- 如果没有指定host参数，则允许网络中的所有主机建立临时访问列表条目，动态访问控制列表包含网络掩码来启动新的网络连接。

4.7 访问控制列表配置要点

- 对于某个协议，可能有多个访问控制列表。通常，一个端口的一个协议，只能够指定一个访问控制列表。
- 对于某些协议，一个端口可以指定两个访问控制列表：一个负责收到的数据，一个负责发出的数据。而某些协议，需要把这两个访问控制列表组合成一个负责进出该端口的数据。
- 假如访问控制列表负责控制接收数据，当路由器接收到数据包，将检查是否满足访问控制列表的条件。假如这个数据包被允许，路由器继续处理这个数据包。如果被拒绝，该数据包将被丢弃。
- 如果访问控制列表是负责控制发出数据，当接收到一个数据包，并发送到了发出端口，路由器将检查访问控制列表的条件是否满足。假如数据包被允许，则传送这个数据包，如果数据包被拒绝，将丢弃这个数据包
- 访问控制列表的放置位置：
 - 访问控制列表可以用于控制数据流，消除不需要的数据流。依赖于访问控制列表放置的位置，可以减少不必要的数据流。如在远离目的端，禁止某些数据流，可以减少使用到达目的端的网络资源。
 - 为了使用访问控制列表的安全特性，至少需要在边界路由器上配置访问控制列表。从外部网络，或者网络控制较少的区域进入网络中更为私有的区域，在这些边界路由器上，可以为路由器的每一个端口的每一个协议配置访问控制列表，使得流入或者流出的数据被过滤
- 访问控制列表放置的规则是
 - 尽量将扩展访问控制列表放置在靠近被拒绝的数据源。标准访问控制列表不能指定目标地址，故需要把标准访问控制列表放置在尽量靠近目标的地方。