网络与系统安全

第三章 网络安全应用基础

黄 玮

温故

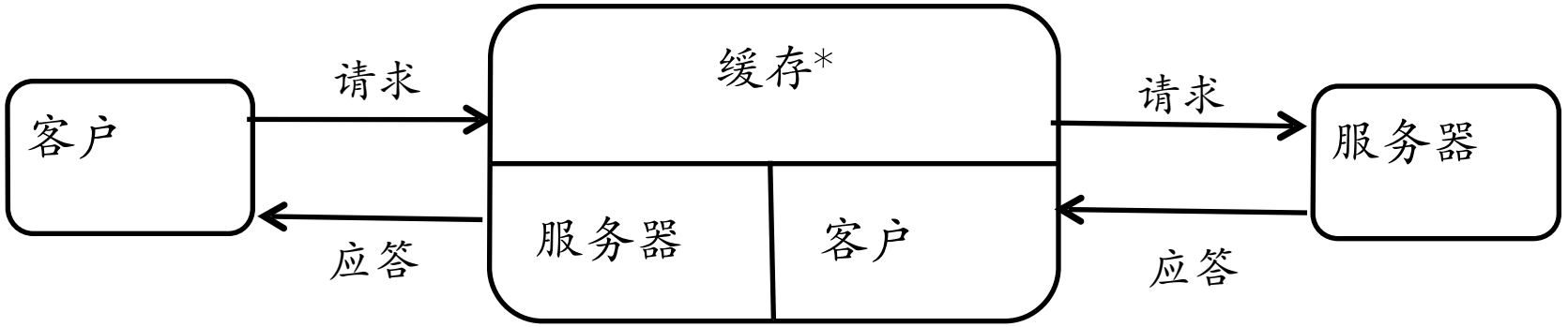
- TCP/IP网络分层模型
- 安全三要素
  - —CIA
- 私有地址
- 公有地址
- 数字标识
  - —网络标识
  - —主机标识

- IP地址不能作为确认攻击者身份的唯一标识
- 源和目的地址都是私有地址的数据包也能在“公网”上传输
- 代理服务的实现形式多种多样
  - —公开协议
  - —私有协议

本章内容提要

- 常见代理服务
  - —HTTP代理
  - —虚拟专用网(VPN)
  - —SOCKS代理
- 高级代理服务
- 代理服务的检测

网络代理的基本原理



代理服务器同时扮演服务器和客户端两种角色

代理服务器是客户与服务器关系的中间人

*可选组件

网络代理的基本类型

- 转发代理
  - —正向代理
  - —最常见
- 开放代理
  - —互联网上人人可访问的转发代理
- 反向代理
  - —将客户端请求转发给后端服务器集群中的某个节点处理并返回处理结果给客户端

转发代理的应用场景

- 过滤
  —内容过滤
- 缓存
- 绕过内容过滤和网络审查
- 日志和嗅探
- 私有网络的网关
- 匿名服务访问

反向代理的应用场景

- 提升加密链接性能
- 负载均衡
- 静态内容缓存
- 压缩（代理）
- 适配低网速客户端
- 安全网关
- 外网发布

网络代理的应用——亦正亦邪

- 正
  - —加密通信数据*
    - 防止通信数据被窃听和篡改
  - —审查网络通信数据*
    - 恶意流量检测和过滤
    - 失泄密行为发现和阻止
  - —改变网络拓扑结构*
    - 跨局域网/异构网络通信

保证通信过程的机密性和完整性

- 邪
  - —隐藏来源IP
  - —绕过网络安全审查/检测机制

威胁网络安全检测、审计机制

网络安全的对抗本质

* 视具体代理服务实现技术而定

本章内容提要

- 常见代理服务
  - —HTTP代理
  - —虚拟专用网(VPN)
  - —SOCKS代理
- 高级代理服务
- 代理服务的检测

HTTP简介

- HTTP协议族
  - —RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1
  - —RFC 2617: HTTP Authentication: Basic and Digest Access Authentication
  - —RFC 2818: HTTP Over TLS
  - —RFC 6265: HTTP State Management Mechanism
  - —RFC 2145 : Use and Interpretation of HTTP Version Numbers - Informational
  - —MIME相关RFC
    - RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289, RFC 2049
- HTTP基本连接过程
  - —建立连接（连接准备、连接）
  - —客户端发送请求/服务器发送响应
  - —关闭连接

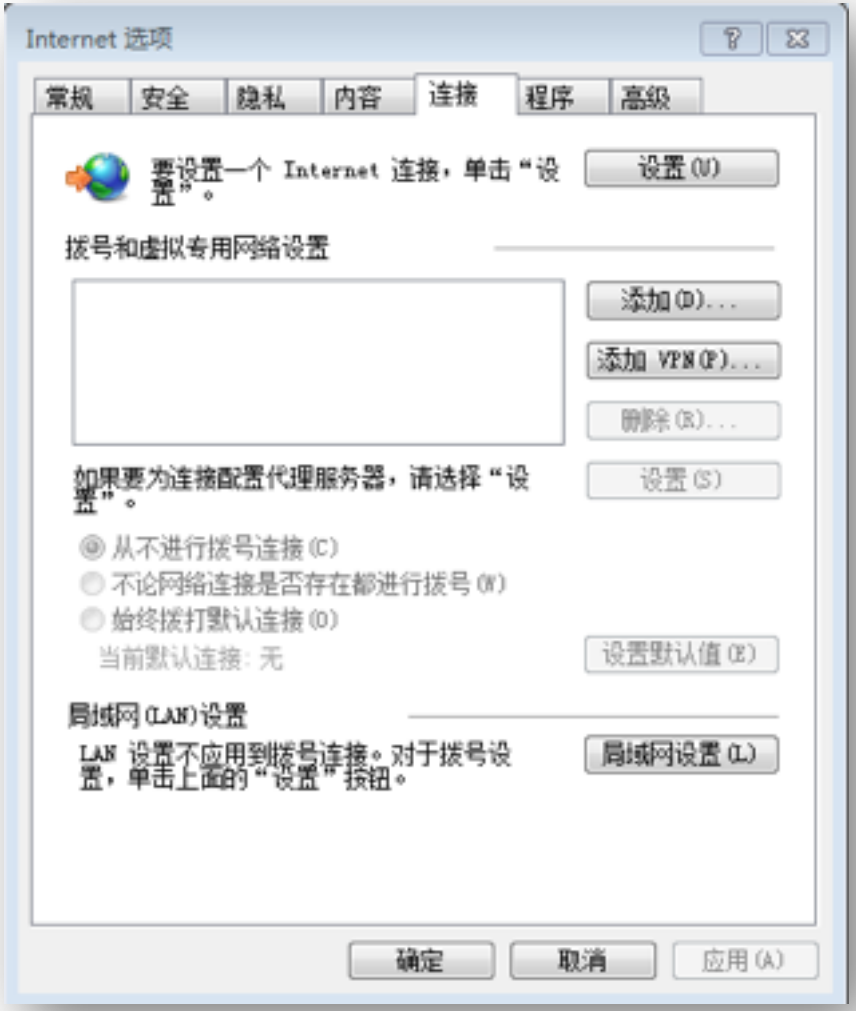
HTTP代理类型

- 正向代理
  - —通常意义上的“代理”
    - 改变通信数据内容*
- 反向代理
  - —面向用户完全透明
    - 对通信内容无修改

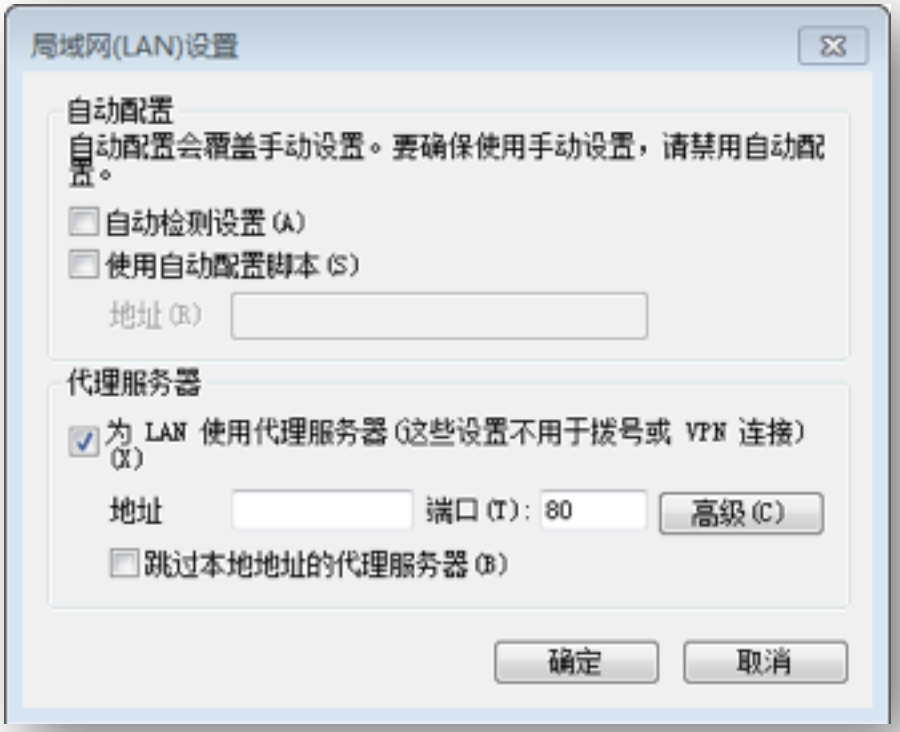
*和HTTP代理的工作模式有关

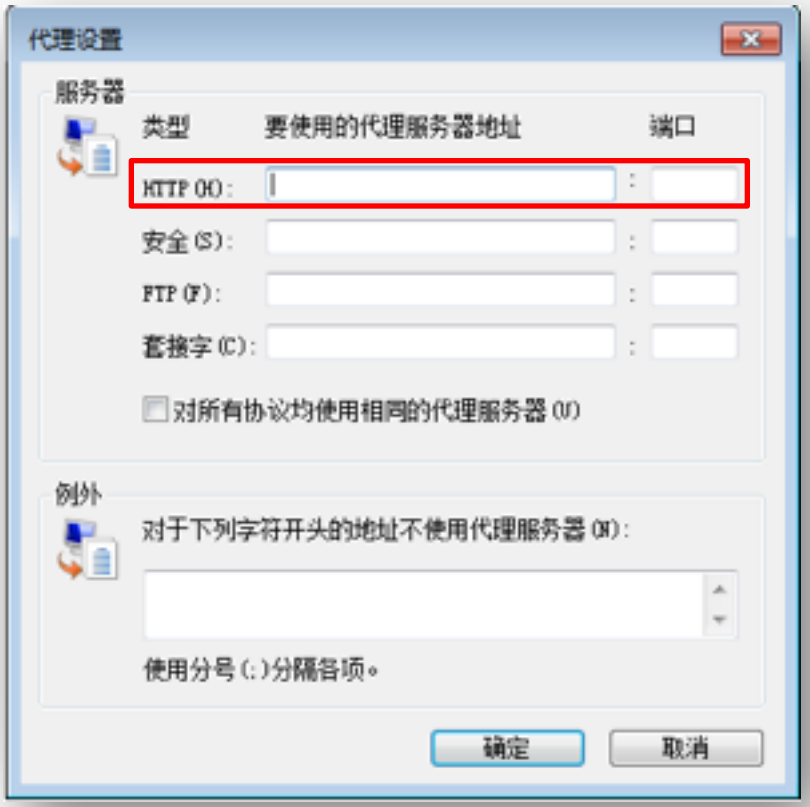
帮助用户访问万维网

HTTP代理的应用


Internet 选项
常规
安全
隐私
内容
连接
程序
高级
要设置一个 Internet 连接，单击“设置”。
设置(U)
拨号和虚拟专用网络设置
添加(D)...
添加 VPN(P)...
删除(R)...
如果要为连接配置代理服务器，请选择“设置”。
设置(S)
从不进行拨号连接(C)
不论网络连接是否存在都进行拨号(W)
始终拨打默认连接(O)
当前默认连接: 无
设置默认值(E)
局域网(LAN)设置
LAN 设置不应用到拨号连接。对于拨号设置，单击上面的“设置”按钮。
局域网设置(L)
确定
取消
应用(A)

HTTP代理的应用


局域网(LAN)设置
自动配置
自动配置会覆盖手动设置。要确保使用手动设置，请禁用自动配置。
自动检测设置(A)
使用自动配置脚本(S)
地址(R)
代理服务器
为 LAN 使用代理服务器(这些设置不用于拨号或 VPN 连接)(X)
地址
端口(T): 80
高级(C)
跳过本地地址的代理服务器(B)
确定
取消


代理设置
服务器
类型
要使用的代理服务器地址
端口
HTTP(H):
安全(S):
FTP(F):
套接字(C):
对所有协议均使用相同的代理服务器(U)
例外
对于下列字符开头的地址不使用代理服务器(N):
使用分号(;)分隔各项。
确定
取消

HTTP代理的主要用途

- 访问受限制的Web站点
  —限制机制：根据客户端来源IP过滤
- 优化Web站点访问速度
  —预先缓存客户端要访问的数据
- 内容审查
  —发现恶意内容并加以过滤阻止

HTTP代理的工作模式

- X-Forwarded-For (XFF)
  - —非RFC标准定义
  - —Squid代理的开发人员最早引入该HTTP消息头
  - —标识客户端真实IP
  - —X-Forwarded-For: client1, proxy1, proxy2
- 匿名代理
  - —不提供X-Forwarded-For字段
- 非匿名代理
  - —提供X-Forwarded-For字段

实际应用中的HTTP代理类型

	*REMOTE_ADDR	*HTTP_VIA	*HTTP_X_FORWARDED_FOR
透明代理	最后一个代理服务器IP	代理服务器IP	客户端真实IP，或（经过多个代理时）遵循XFF标准
普通匿名	最后一个代理服务器IP	代理服务器IP	部分遵循XFF标准（隐藏客户端真实IP）
欺骗代理	代理服务器IP	代理服务器IP	伪造经过的代理服务器IP地址列表
高匿名代	代理服务器IP	无数值或不显示	无数值或不显示

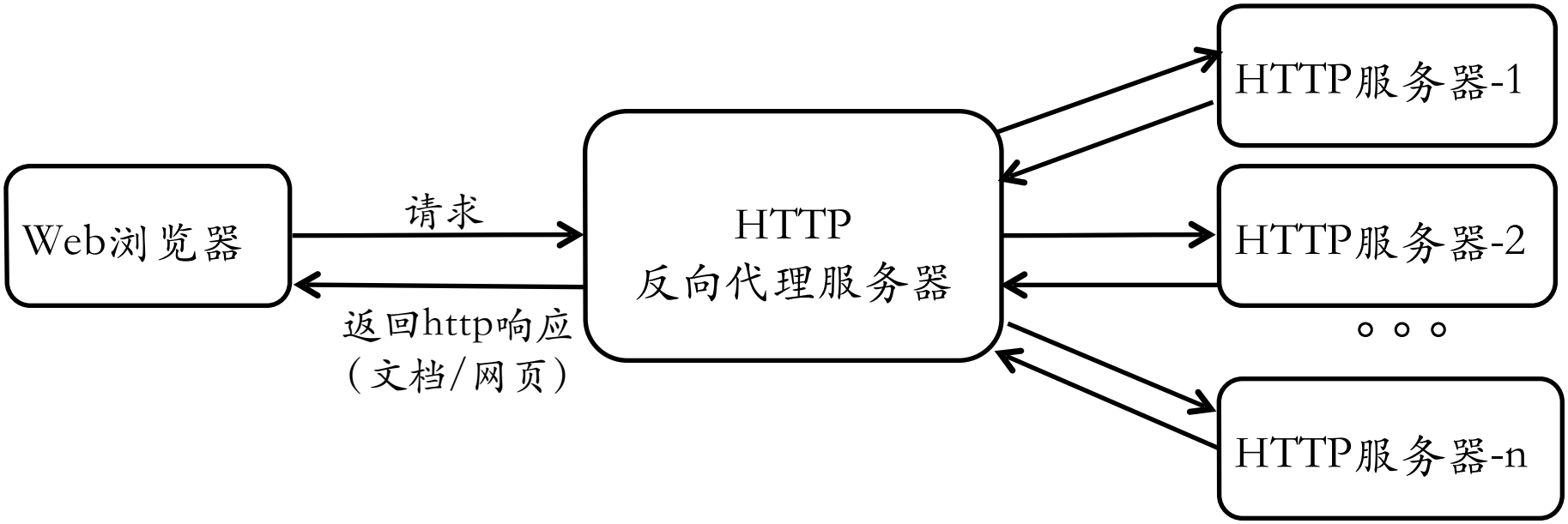
在线检查你当前所使用的HTTP代理类型：http://www.adamek.biz/php.php

*以PHP编程接口为例

代理地址实例

IP(怎样使用代理)	Port 端口	国家/地区(搜索关键字用空格隔开.) 美国 搜索地区	transparent:透明 anonymous:匿名 high anonymity:高度匿名	Last Test最后测试
207.7.126.74	80	美国	high-anonymous	2011-09-20 13:38:17 验证
120.203.215.11	80	江西省 移动	high-anonymous	2011-09-20 13:21:40 验证
114.127.208.77	8000	印度尼西亚	high-anonymous	2011-09-20 12:57:19 验证
74.52.18.181	3128	美国 ThePlanet机房	transparent	2011-09-20 12:39:05 验证
216.155.139.115	3128	美国	high-anonymous	2011-09-20 12:58:05 验证
114.127.208.79	8000	印度尼西亚	high-anonymous	2011-09-20 10:09:30 验证
158.130.13.94	8909	美国 宾夕法尼亚大学	high-anonymous	2011-09-20 09:22:13 验证
205.213.195.70	8080	美国	anonymous	2011-09-20 11:57:30 验证
173.10.184.67	8080	美国	anonymous	2011-09-20 10:58:00 验证
200.123.4.72	8080	秘鲁	anonymous	2011-09-20 09:57:42 验证

按照规则从指定的服务器取内容返回给客户端



HTTP反向代理的主要用途

- 内网对外服务的堡垒主机
  - —负载均衡
  - —缓冲
- 内容小偷网站
  - —黑帽SEO

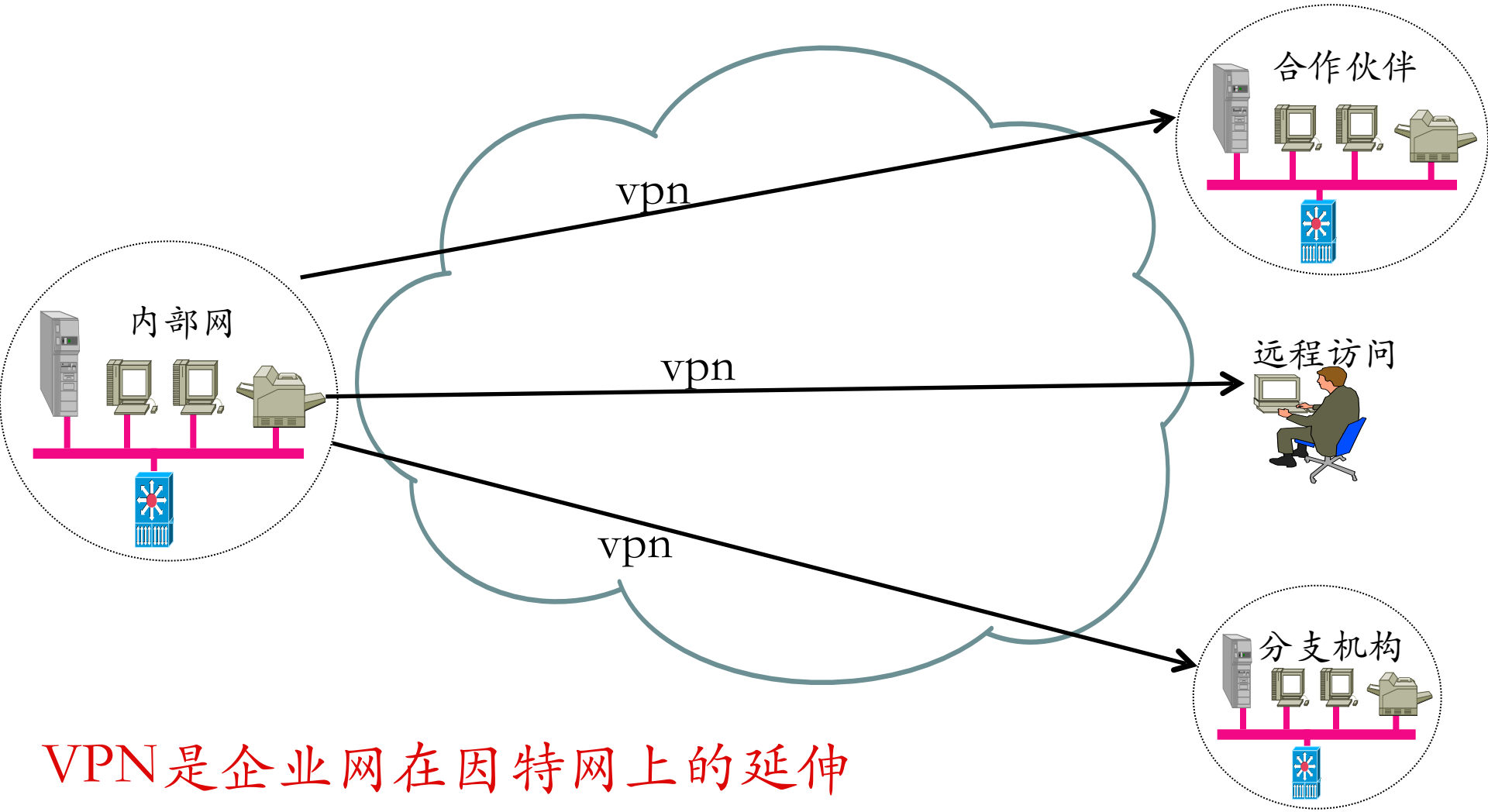
本章内容提要

- 常见代理服务
  - —HTTP代理
  - —虚拟专用网(VPN)
  - —SOCKS代理
- 高级代理服务
- 代理服务的检测

虚拟专用网——VPN简介

- VPN是企业网在因特网等公共网络的延伸
- VPN通过一个私有的通道来创建一个安全的私有的连接

VPN的典型应用



VPN是企业网在因特网上的延伸

虚拟专用网的主要用途

- 保障通信过程的机密性和完整性
- 实现自主可控的跨网络专用通信网
  - —使局域网的拓扑延伸到互联网上的任意一个终端
    - 远程访问局域网资源的可行技术手段
  - —相比较于物理链路专用的通信网解决方案成本更低

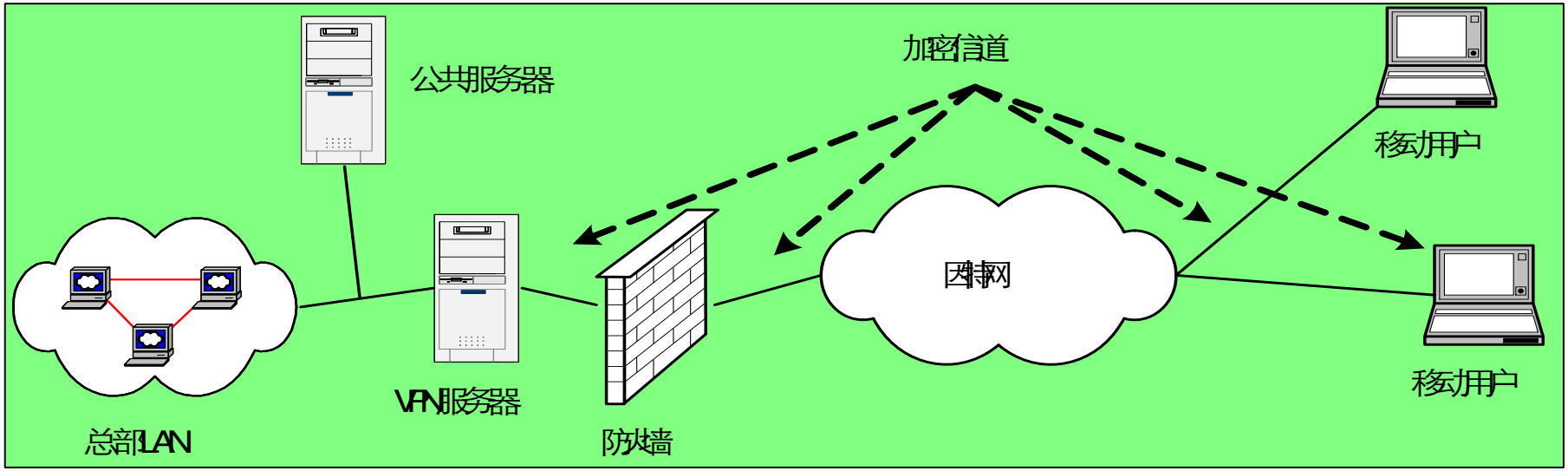
虚拟专用网的分类

- 按应用类型分类
  - —Access VPN
  - —Intranet VPN
  - —Extranet VPN
- 按实现的层次分类
  - —二层隧道 VPN
  - —三层隧道 VPN
  - —应用层隧道VPN：SSL VPN

- 又称为拨号VPN
  - —VPDN：Virtual Private Dial Network
  - —企业员工或企业的小分支机构通过公网远程拨号的方式构筑的虚拟网
- 技术实现
  - —模拟、拨号、ISDN、数字用户线路(XDSL)、移动IP和电缆技术

Access VPN

- 用户通过本地的ISP登录到因特网上，并在现在的办公室和公司内部网之间建立一条加密通道

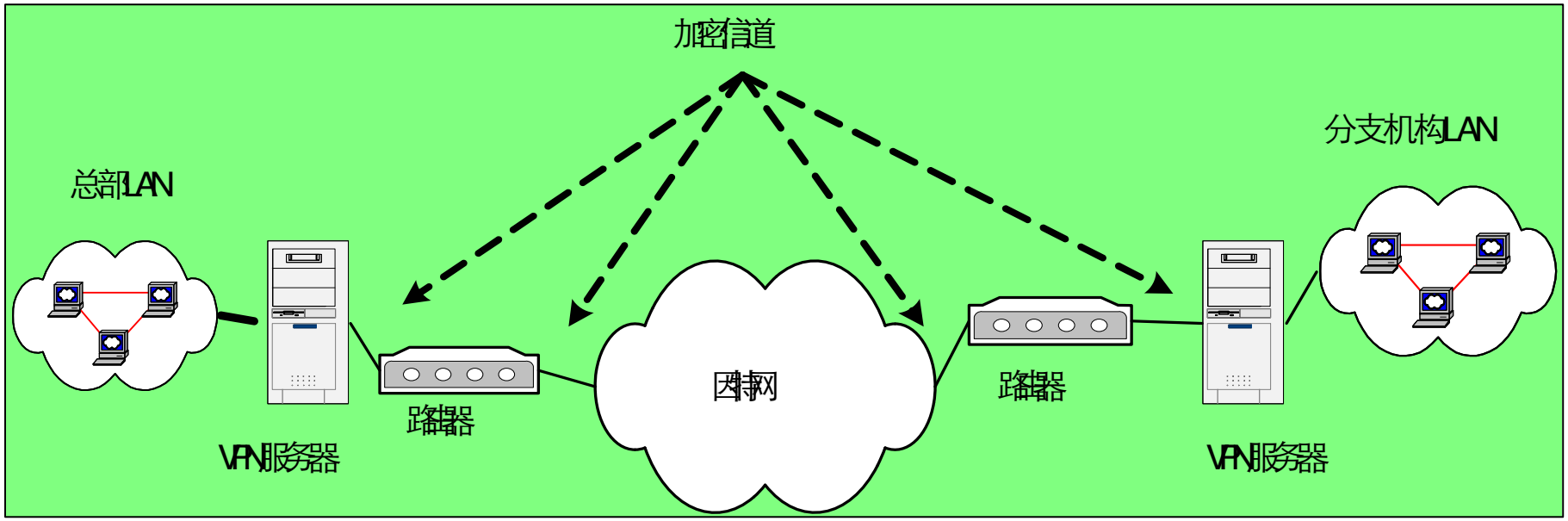


Access VPN的优点

- 减少用于相关的调制解调器和终端服务设备的资金及费用，简化网络
- 显著降低远距离通信的费用
- 极大的可扩展性，简便的对加入网络的新用户进行调度
- 远端验证拨入用户服务基于标准，基于策略功能的安全服务

Intranet VPN

- 又称内部网VPN
- 企业的总部与分支机构间通过公网构筑的虚拟网

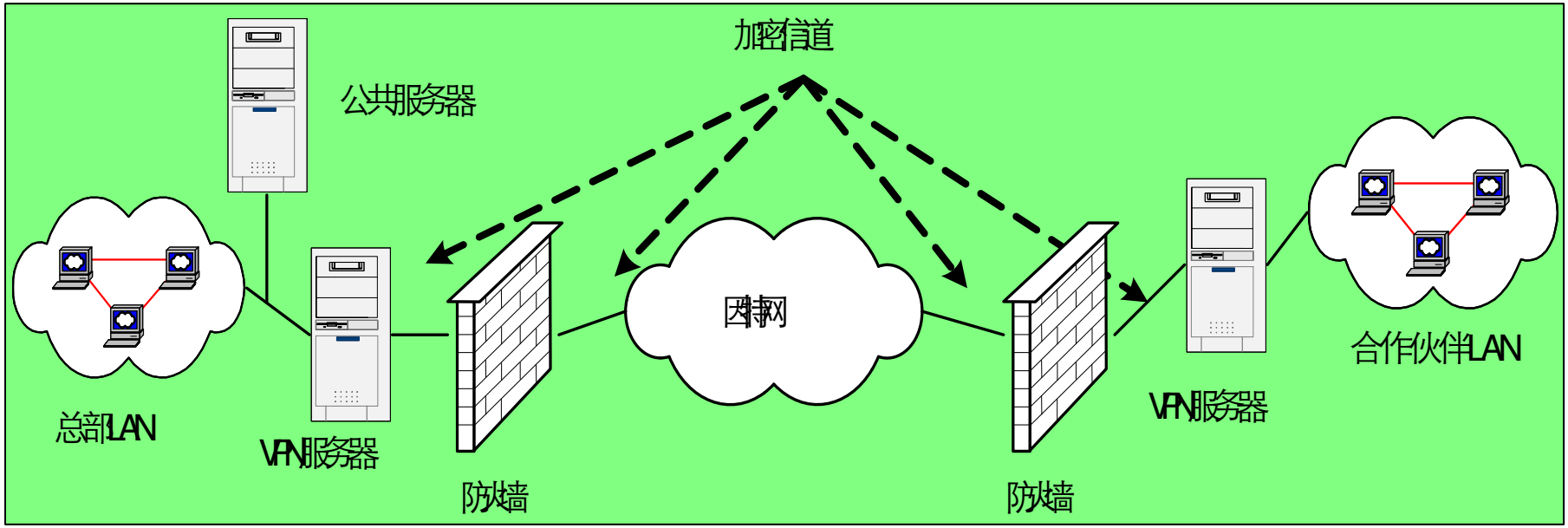


Intranet VPN的优点

- 减少WAN带宽的费用
- 能使用灵活的拓扑结构
- 新的站点能更快，更容易的被连接
- 通过设备供应商WAN的连接冗余，可以延长网络的可用时间

Extranet VPN

- 又称外联网VPN
- 企业间发生收购、兼并或企业间建立战略联盟后，使不同企业网通过公网来构筑的虚拟网



Extranet VPN的优点

- 能容易的对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问VPN相同的架构和协议进行部署
- 主要的不同是接入许可，外部网的用户被许可只有一次机会连接到其合作人的网络

二层隧道协议

- L2F
  - —Layer 2 Forwarding
- PPTP
  - —Point To Point Tunnel Protocol
- L2TP
  - —Layer 2 Tunnel Protocol
  - —IETF标准：RFC 2661

三层隧道协议

- GRE
  —General Routing Encapsulation
- IPSec
  —IP Security Protocol

应用层隧道协议——SSL VPN

- 安全性
  - —与IPSEC VPN相当
  - —支持访问控制
- 易用性
  - —客户端只需要有支持ssl的浏览器即可
  - —客户端基本零配置
  - —非常适合远程用户访问企业内部网
- 局限性
  - —*仅支持Web应用

VPN设计原则

- 安全性
  - —隧道与加密
  - —数据验证
  - —用户验证
  - —防火墙与攻击检测
- 可靠性
- 经济性与扩展性

主流VPN协议比较(1/2)

	PPTP	L2TP/IPSec	OPENVPN
背景	• 基于PPP的基本VPN协议 • 微软平台上最早支持的VPN协议 • 默认未考虑加密或认证问	• RFC3193及相关RFC标准	• 开源VPN解决方案
数据加密	• PPP负载使用微软点到点加密协议（MPPE） • MPPE实现RSA RC4加密算法，最大支持128bit密	• L2TP负载使用标准IPSec协议加密 • RFC 4835规定使用3DES或者AES	• 使用OpenSSL加密库 • 支持3DES、AES、RC5、
速度	• 使用128bit密钥加密时性能略高于使用256bit密钥加密	• 数据封装2次，导致性能下降	• UDP模式下性能达到最佳

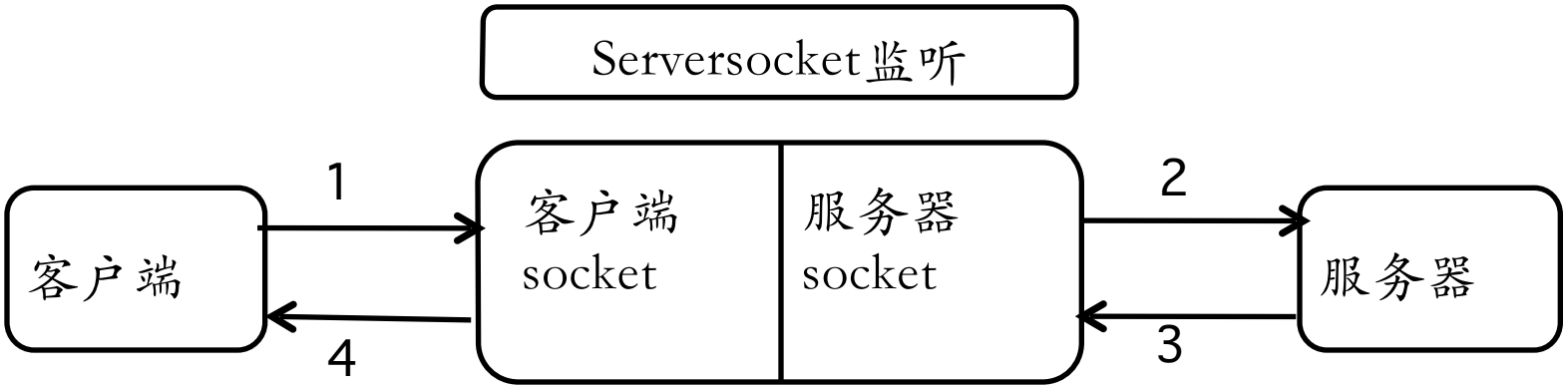
主流VPN协议比较(2/2)

	PPTP	L2TP/IPSec	OPENVPN
安全漏洞	• 微软的PPTP实现有严重安全漏洞 • MSCHAP-v2容易遭受基于字典的暴力破解	• 未发现严重漏洞 • 配合使用高强度加密算法（如AES）时安全性	• 未发现严重漏洞 • 配合使用高强度加密算法（如AES）时安全性
客户端兼容性	•Windows •Mac OSX •Linux •Apple iOS	•Windows •Mac OSX •Linux •iOS	•Windows •Mac •Linux •Android
综合评分	★☆☆☆☆	★★★★☆	★★★★★

本章内容提要

- 常见代理服务
  - —HTTP代理
  - —虚拟专用网(VPN)
  - —SOCKS代理
- 高级代理服务
- 代理服务的检测

SOCKS代理原理



SOCKS代理的应用

- 主要用途
  - —SOCKS是一种网络传输协议，主要用于客户端与服务器之间通讯的中间传递
- 实际应用
  - —电子邮件
  - —新闻组软件
  - —网络传呼ICQ
  - —网络聊天QQ
  - —使用代理服务器上联众打游戏

常见代理服务小结

- 使用开放代理要谨慎
  - —避免敏感数据被嗅探
  - —避免重要数据被篡改
- 一般情况下的代理安全性排序
  - —VPN ≥Socks代理 > HTTP代理

本章内容提要

- 常见代理服务
  - —HTTP代理
  - —虚拟专用网(VPN)
  - —SOCKS代理
- 高级代理服务
- 代理服务的检测

匿名通信

- 匿名的基本概念
- 匿名保护的形式
- 匿名通信面临的技术性攻击
- 匿名通信的实现

匿名的基本概念

- 定义

  ——一个对象在一组对象的集合（即匿名集合，Anonymityset）中不可识别的状态

- 匿名集合

  ——指发生某个行为（如发送一封电子邮件或者访问某个网站）的可能实体（如用户）的集合

  ——匿名集的概念是研究匿名技术的基础

匿名的基本概念

- 匿名行为

  —借助于其他 实体的行为来隐藏自己的行为

  —匿名集合越大，分布越均匀，匿名性就越强

- 不可关联性

  —两个或多个对象（如实体、消息、事件、行为等）之间的不可关联 性是指系统中的这些对象，相对于其先验知识的关联性来说，其关联性没有发生变化

  —攻击发生前后，对象可被关联的概率保持不变

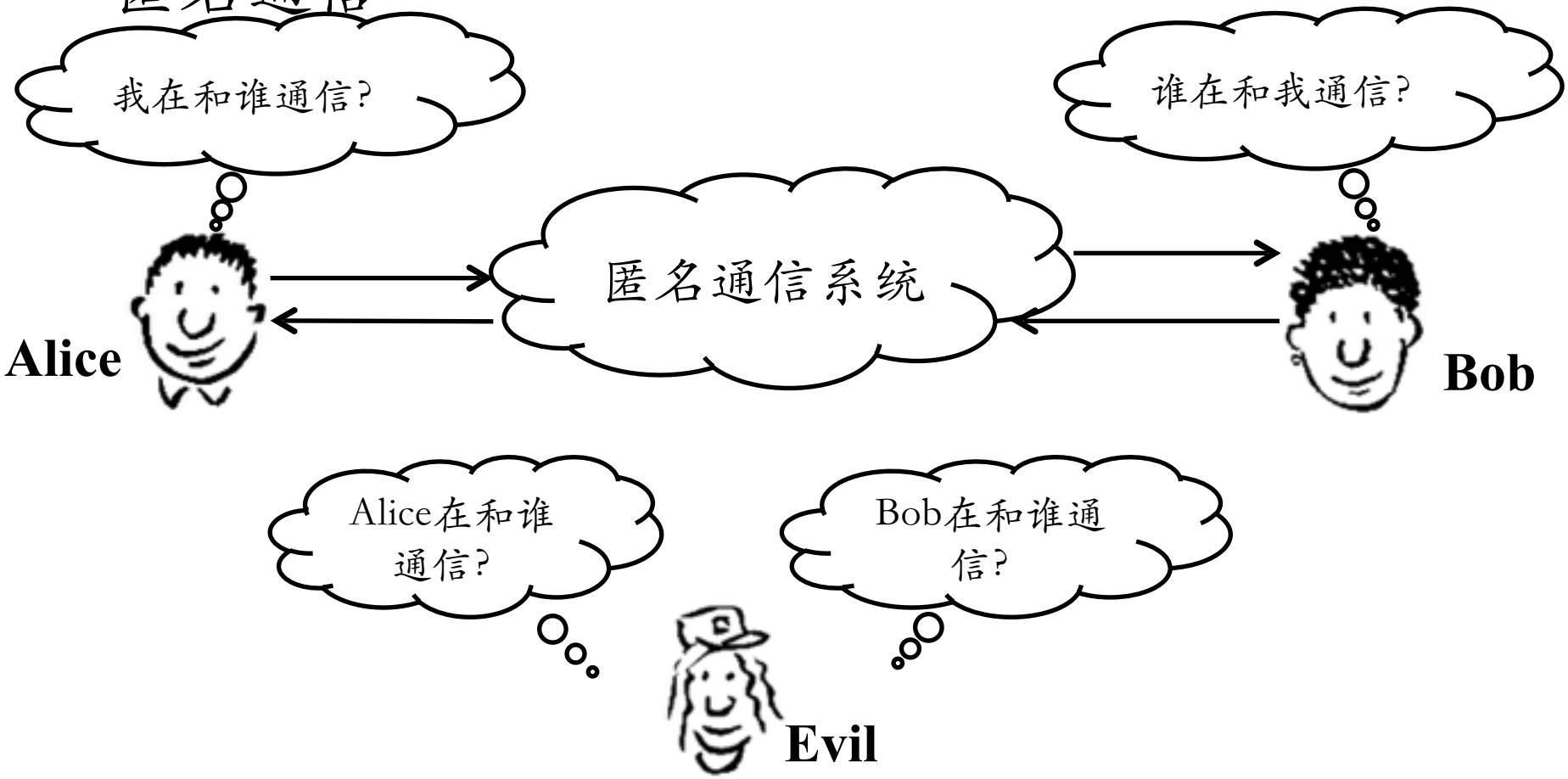
  —不可关联性 → 匿名性，但反之不成立!

匿名的基本概念

- 不可观察性
  - —不能从发送或接收事件集合中分辨出某个发送或接收事件
  - —不可观察性 → 匿名性，但反之不成立！
- 假名
  - —对象使用假名作为其身份标识，假名与对象之间具有不可关联性，是实现 匿名的一种方法
  - —使用不变的假名可以建立问责制和声誉机制，防止匿名系统被滥用

匿名的基本概念

- 匿名通信



匿名通信要研究的问题

- 通信系统中的发送者和接收者的身份信息也是机 密的情况
- 一个匿名系统的攻击者希望得到的是“谁和谁”在通信，甚至要控制或破坏通信过程

匿名保护的形式

- 发送者匿名

  —保护通信发起者的身份标识

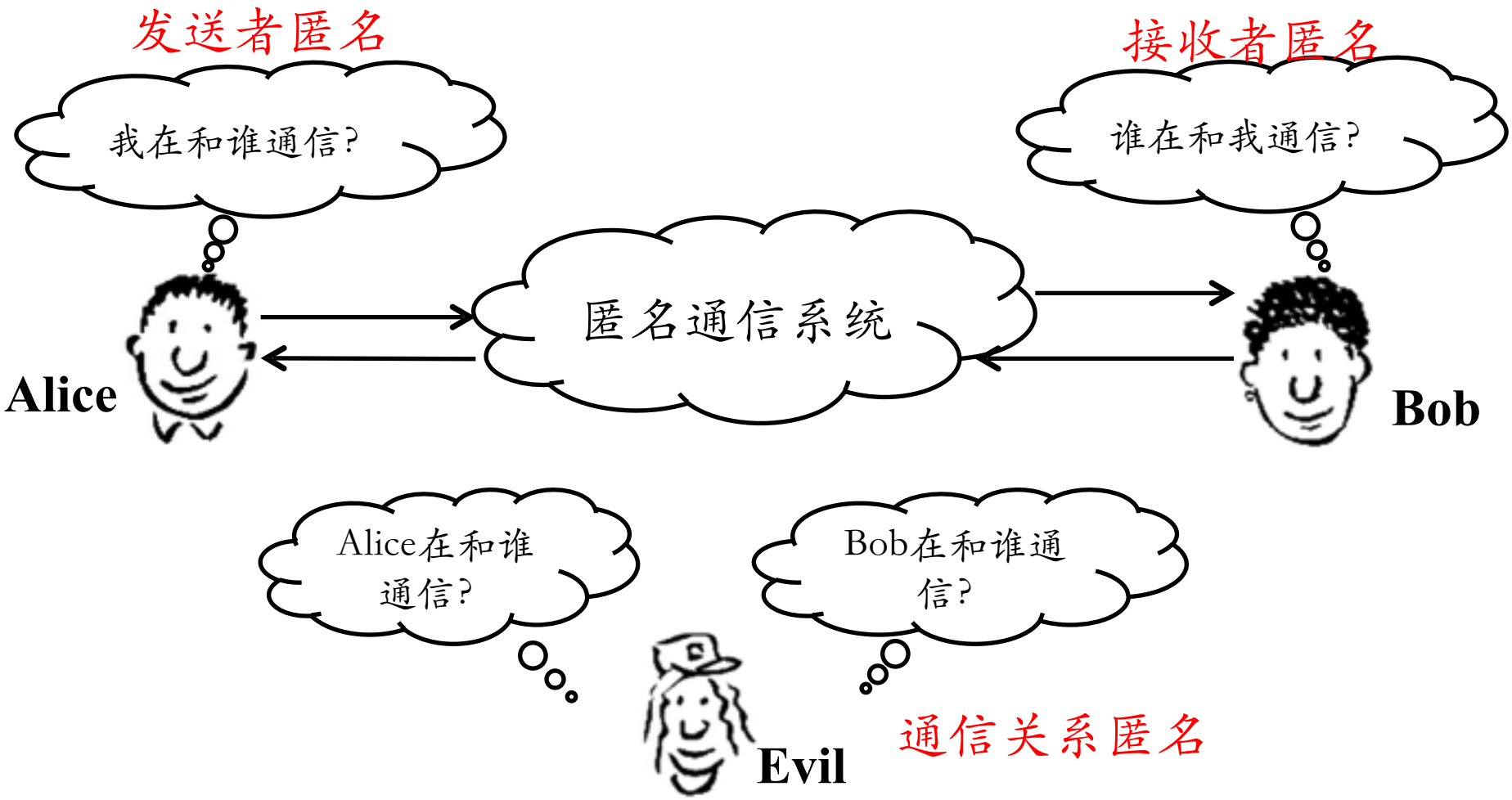
- 接收者匿名

  —保护通信响应者的身份标识

- 通信关系匿名

  —保护通信关系不被攻击者观察到，使发送者和接收者无法被关联起来

匿名保护形式的含义


发送者匿名
接收者匿名
我在和谁通信?
谁在和我通信?
匿名通信系统
Alice
Bob
Alice在和谁通信?
Bob在和谁通信?
Evil
通信关系匿名

匿名通信面临的技术性攻击

- 流量形状攻击
  - —通信模式攻击
  - —消息频度攻击
  - —报文计数攻击
- 交集攻击
- 重放攻击
- 刷新攻击
- 时间攻击

匿名通信的实现

- 代理方法
- MIX-NET
- Crowds
- Tarzan
- 洋葱路由

匿名通信的实现——代理方法(1/2)

- 代理方法的原理
  - —前述匿名代理原理
- 代理分类
  - —匿名代理
  - —假名代理
  - —MIX增强匿名代理

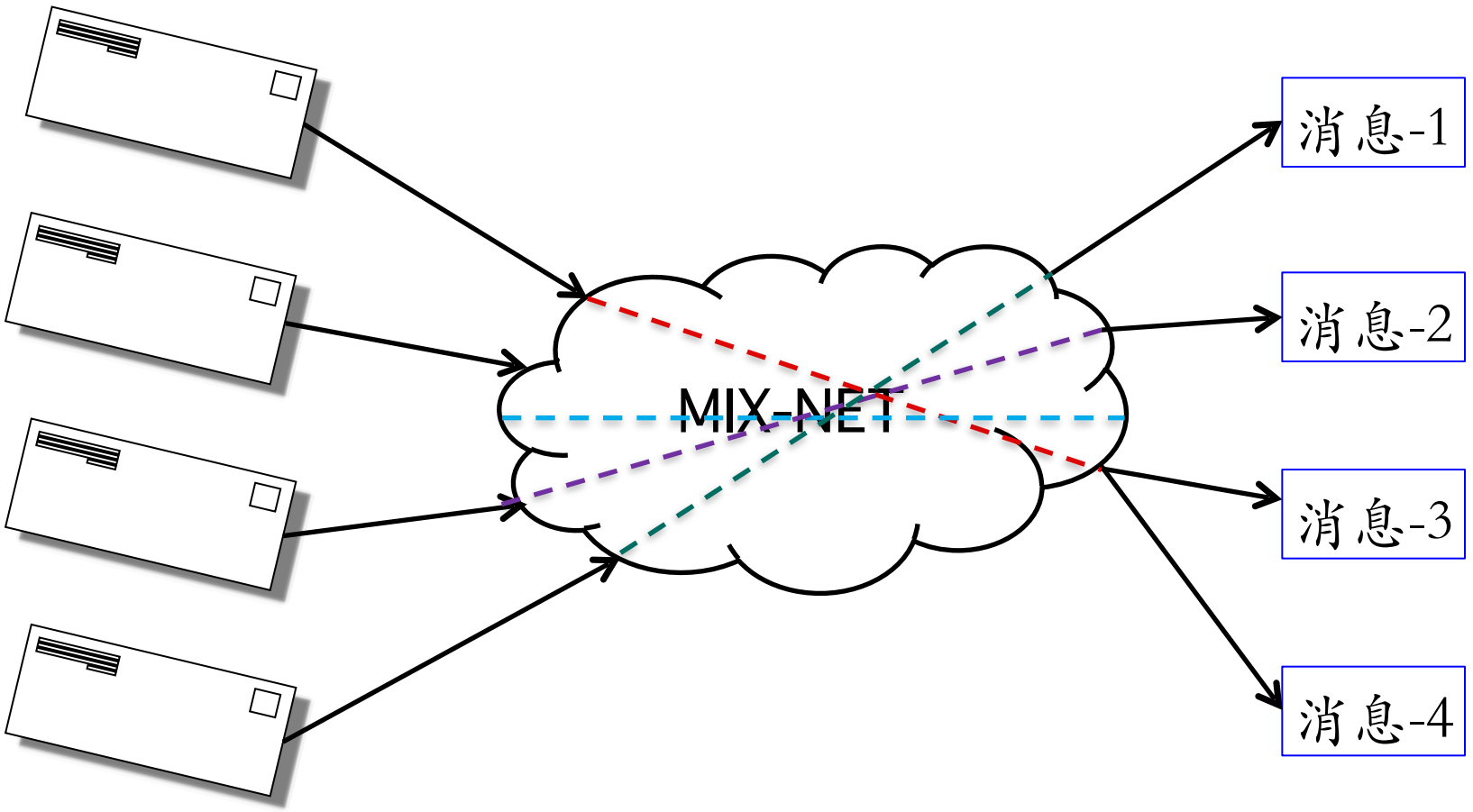
匿名通信的实现——代理方法（2/2）

- 代理方法的优点
  - —发送方匿名的协议简单
  - —高效性
- 代理方法的缺点
  - —安全性上有明显不足
    - 用户身份对代理来说不是保密的，因而要求代理必须是可信任的
    - 采用单点代理实现方法易遭到攻击者的控制和跟踪
    - 用户接入匿名或假名代理采用明文形式，攻击者易于进行流量分析
    - 匿名代理需要做过滤操作，易于成为系统瓶颈

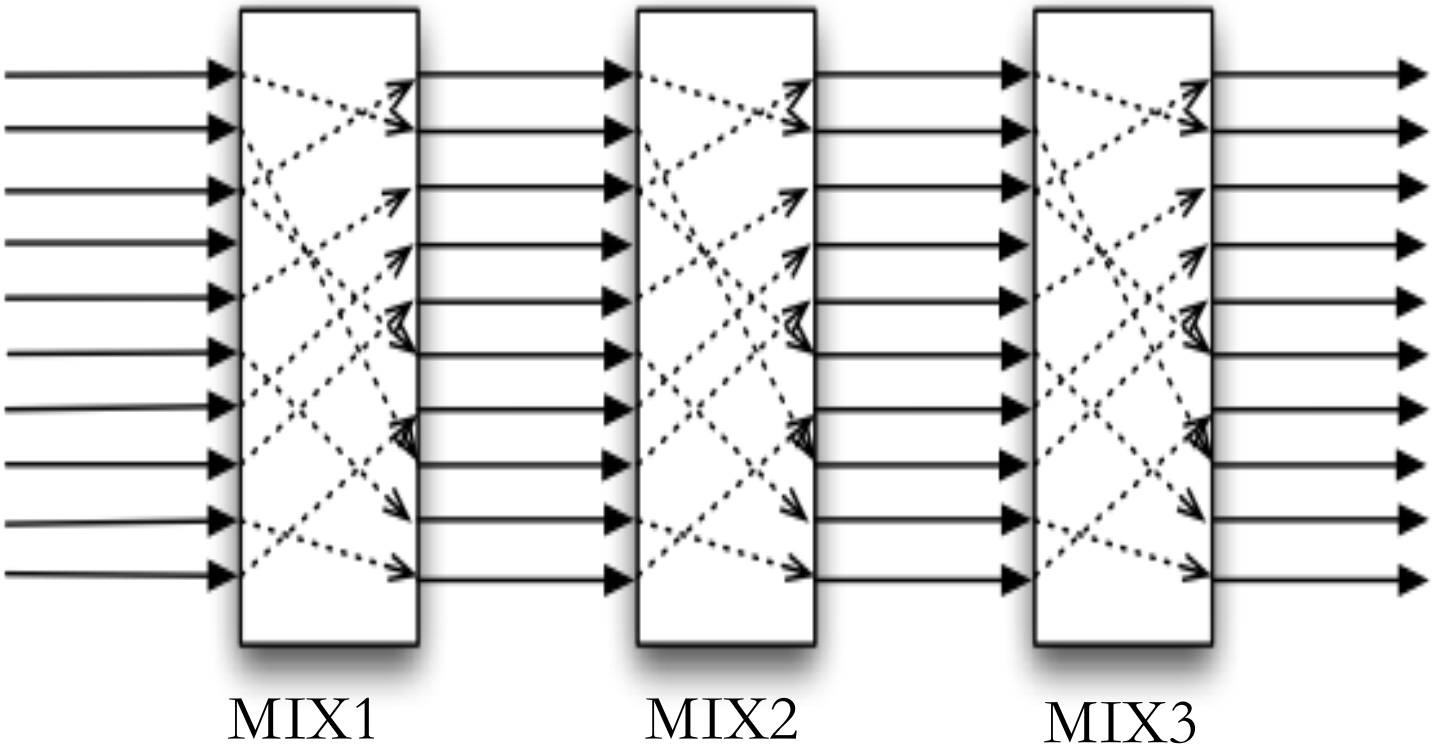
匿名通信的实现——MIX-NET(1/3)

- 基本思想
  - —MIX节点接收消息并处理
    - 通过加密或填充等手段修改消息的外观
    - 通过延迟或重排序等手段来修改消息的顺序
  - —实现隐藏输入输出对应关系的方式输出消息
    - 保证攻击者无法准确推断通信参与者的通信关系
  - —多台MIX服务器可以以级联或网络的形式进行连接

匿名通信的实现——MIX-NET(2/3)



匿名通信的实现——MIX-NET(3/3)

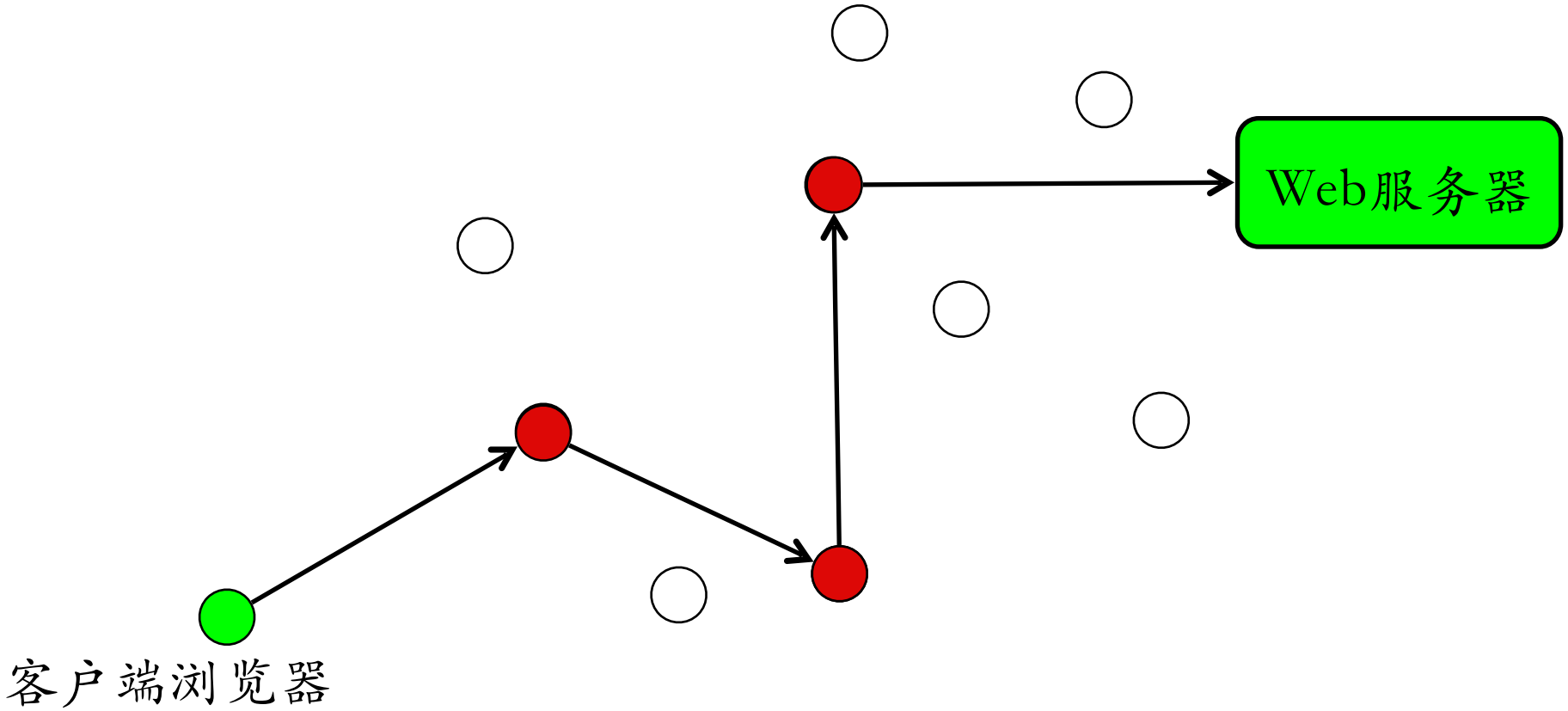


只要有一台服务器正常工作就可以保证系统的匿名性

匿名通信的实现——Crowds(1/2)

- 基于P2P网络结构思想构建的匿名通信网络
  - —史上最早
  - —消息在P2P网络节点之间随机转发
- 使用可信第三方服务器作为crowd会员信息中心节点服务器
- 提供两种匿名保护机制
  - —发送者匿名
  - —通信关系匿名

匿名通信的实现——Crowds(2/2)

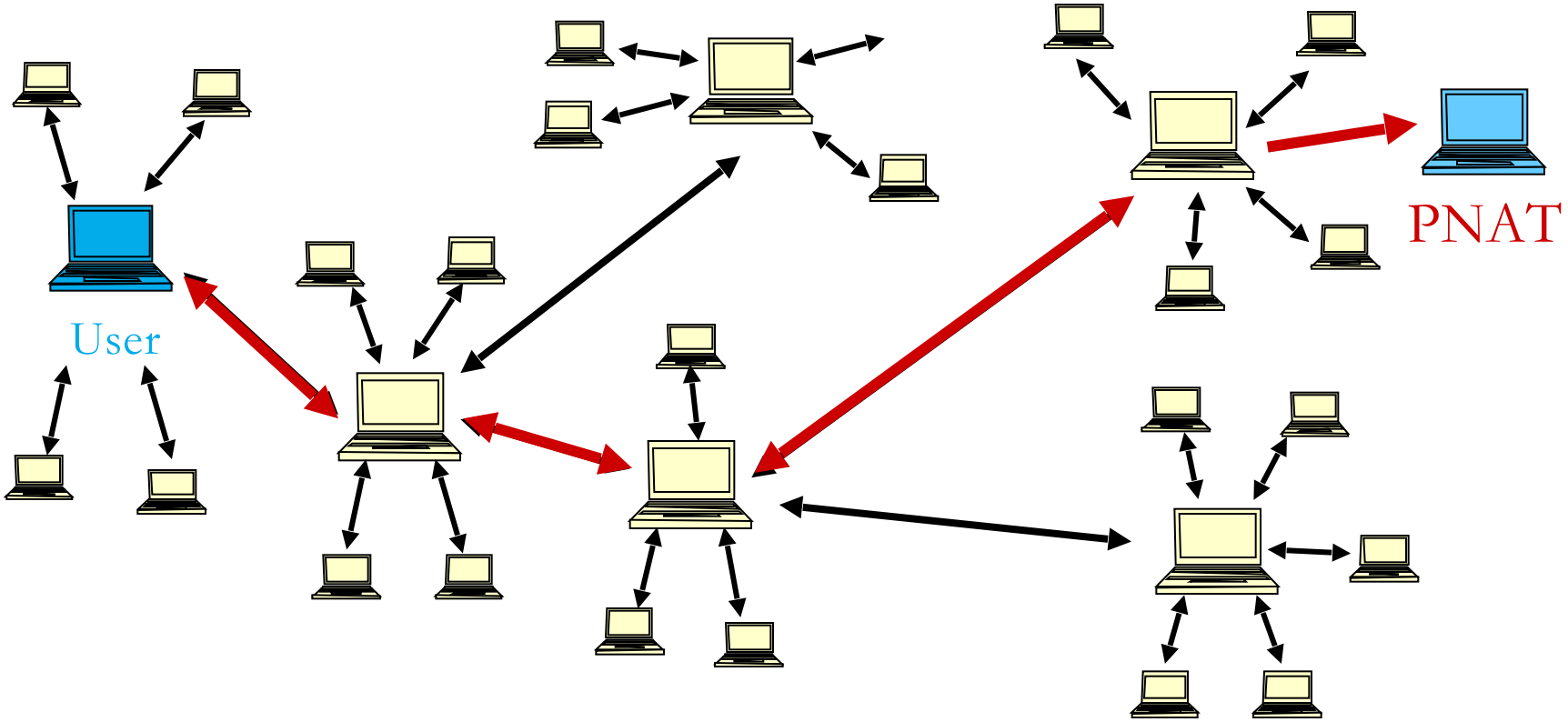


消息在不同服务器之间随机转发，最终发送给目的节点

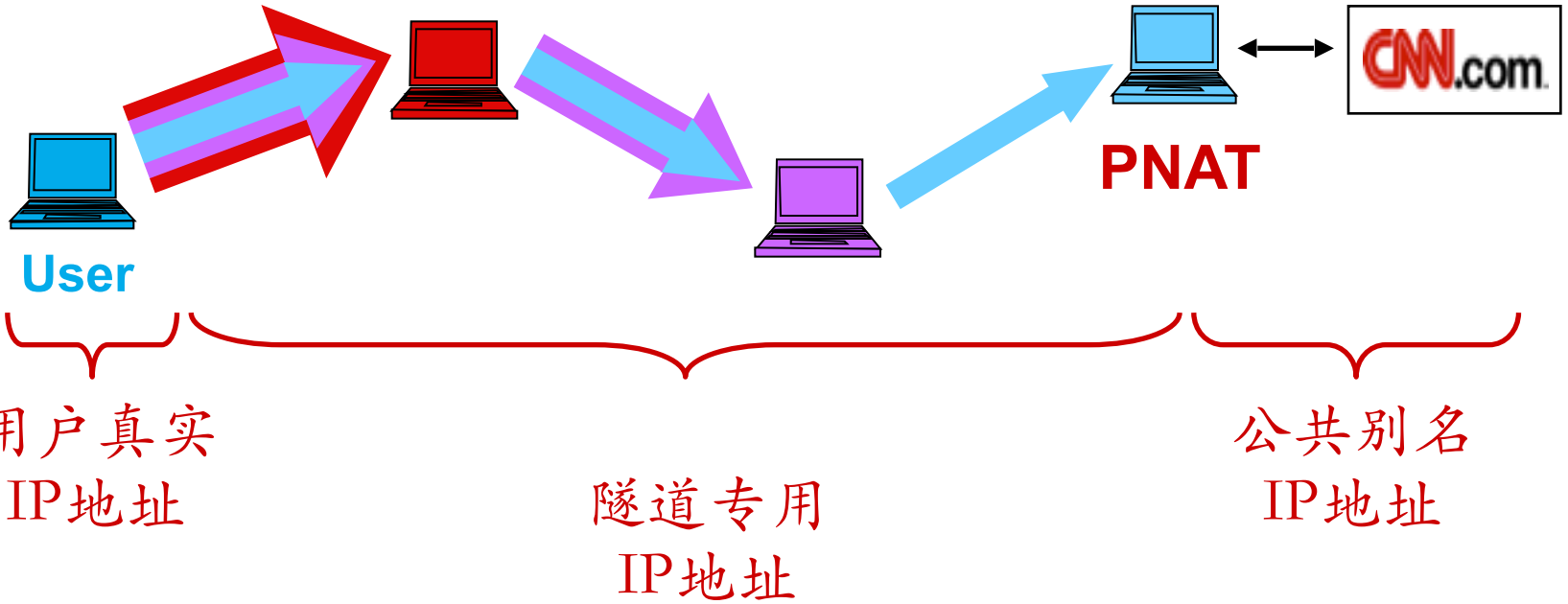
匿名通信的实现——Tarzan（1/3）

- Tarzan在英文中的意思为“泰山”
- Tarzan是一个P2P的匿名IP叠加网络，它通过数据多层加密和消息多跳路由来实现匿名性。
- Tarzan将mix-net的匿名方法扩展到P2P环境中，结点之间通过中继结点序列（这一序列结点构成一条隧道）来通信。
- 提供3种匿名保护机制
  - —发送者匿名
  - —接收者匿名
  - —关系匿名

匿名通信的实现——Tarzan（2/3）



匿名通信的实现——Tarzan（3/3）



匿名通信的实现——洋葱路由

- 匿名传输代理服务器Tor是基于洋葱路由
  - —用户在本机运行一个洋葱代理服务器，这个代理周期性地与其他Tor交流，从而在Tor网络中构成虚拟环路
- Tor是在7层协议栈中的应用层进行加密
- 每个（洋葱）路由器间的传输都经过对称密钥来加密，形成有层次的结构

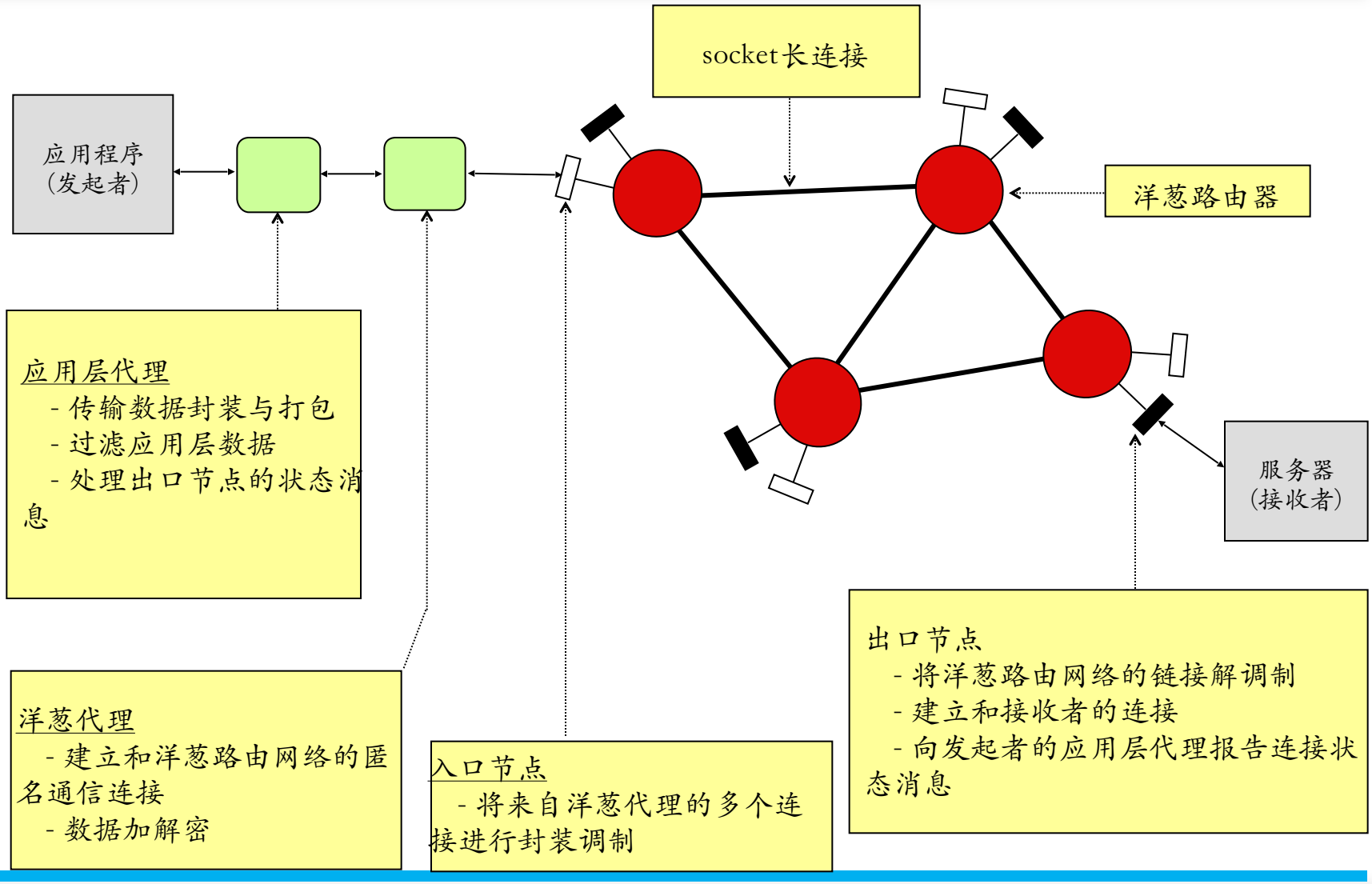
洋葱路由——Onion routing

- 一个通用可用于如Internet开放式网络上的匿名通信体系
- 通过适当的代理支持多类的应用如：HTTP,FTP,SMTP…
- 应用数据通过动态建立的匿名连接传输
- 具有分布式，容错，安全等特性

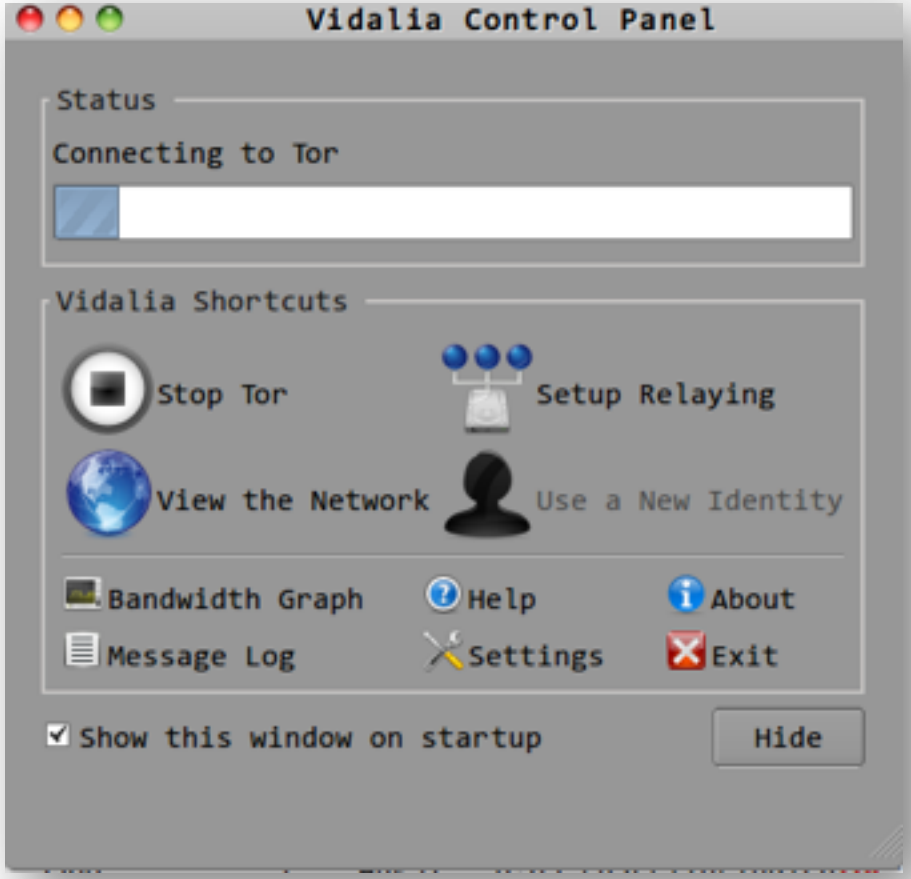
洋葱路由——网络设置和操作

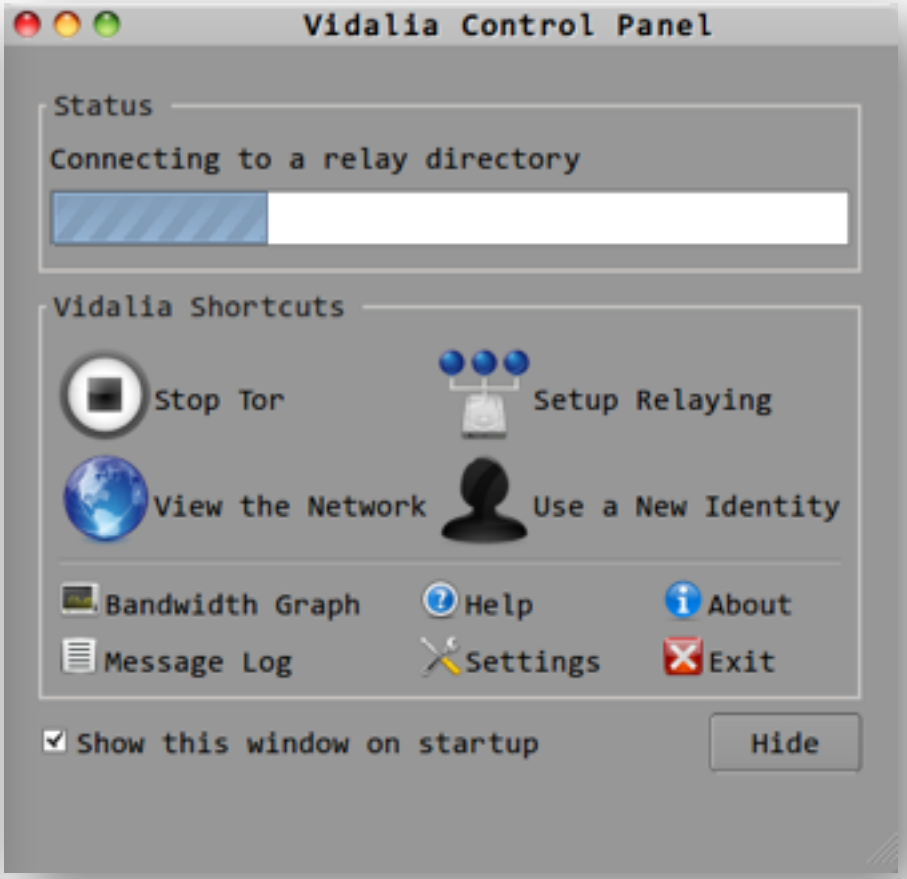
- 在邻居路由器间长期保持的socket连接
- 一个连接上的两邻居采用两个DES加密key，每个方向一个确保通信安全
- 多个匿名连接可以复用在一个连接上，这时每个匿名连接分配一个ACI标识（局部性的标识）
- 消息类似ATM传输，分成48bytes定长信元。信元用DES加密。传输中来自不同连接的信元mix复用，但保持连接有序

洋葱路由——总体架构

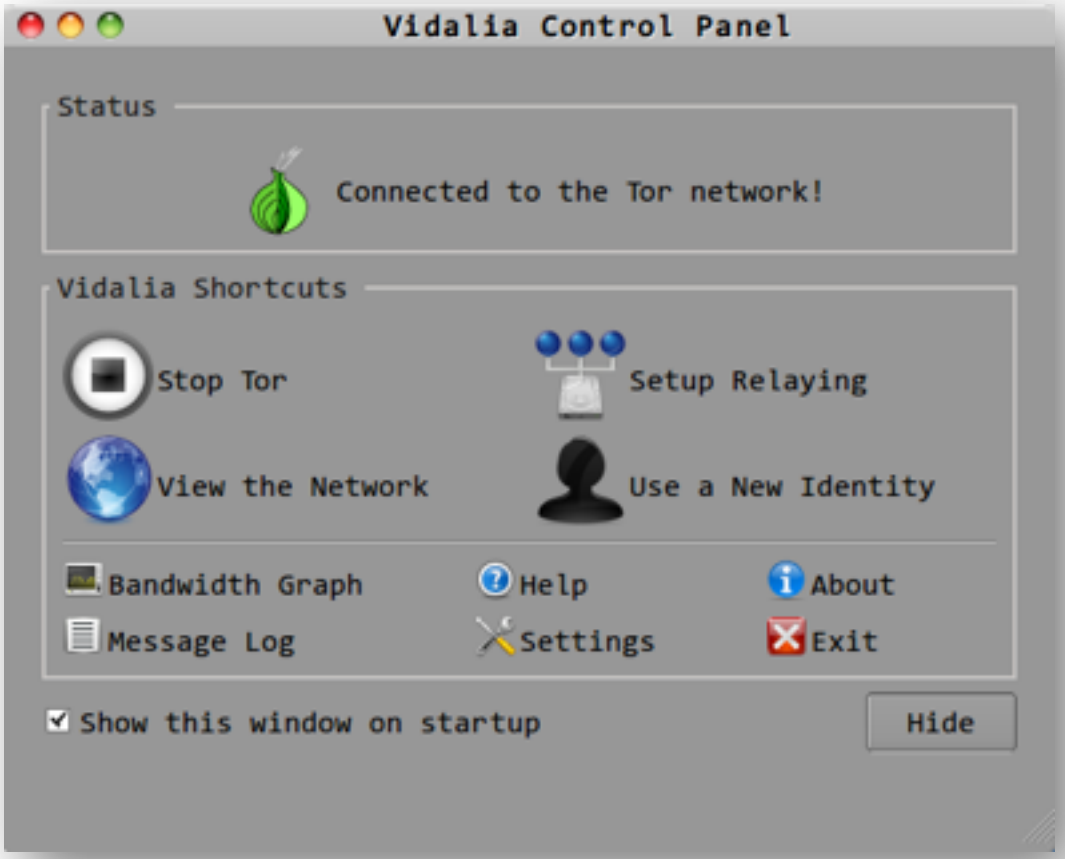

socket长连接
应用程序
(发起者)
洋葱路由器
服务器
(接收者)
应用层代理
- 传输数据封装与打包
- 过滤应用层数据
- 处理出口节点的状态消息
洋葱代理
- 建立和洋葱路由网络的匿名通信连接
- 数据加解密
入口节点
- 将来自洋葱代理的多个连接进行封装调制
出口节点
- 将洋葱路由网络的链接解调制
- 建立和接收者的连接
- 向发起者的应用层代理报告连接状态消息

洋葱路由应用演示(1/4)

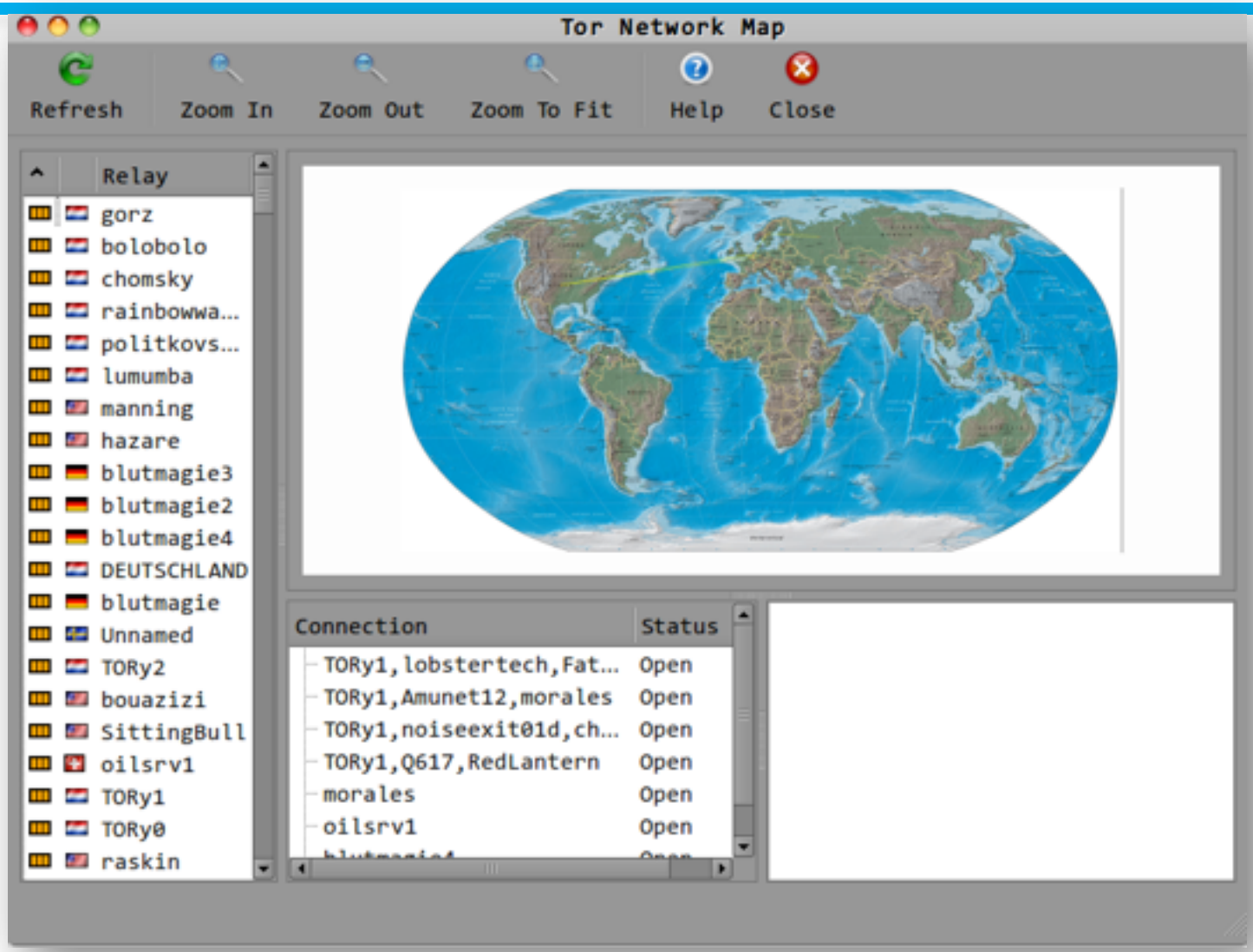

Vidalia Control Panel
Status
Connecting to Tor
Vidalia Shortcuts
Stop Tor
Setup Relaying
View the Network
Use a New Identity
Bandwidth Graph
Help
About
Message Log
Settings
Exit
Show this window on startup
Hide


Vidalia Control Panel
Status
Connecting to a relay directory
Vidalia Shortcuts
Stop Tor
Setup Relaying
View the Network
Use a New Identity
Bandwidth Graph
Help
About
Message Log
Settings
Exit
Show this window on startup
Hide

洋葱路由应用演示(2/4)


Vidalia Control Panel
Status
Connected to the Tor network!
Vidalia Shortcuts
Stop Tor
Setup Relaying
View the Network
Use a New Identity
Bandwidth Graph
Help
About
Message Log
Settings
Exit
Show this window on startup
Hide

洋葱路由应用演示(3/4)


Tor Network Map
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Relay
gorz
bolobolo
chomsky
rainbowwa...
politkovs...
lumumba
manning
hazare
blutmagie3
blutmagie2
blutmagie4
DEUTSCHLAND
blutmagie
Unnamed
TORy2
bouazizi
SittingBull
oilsrv1
TORy1
TORy0
raskin
Connection
Status
TORy1,lobstertech,Fat...
Open
TORy1,Amunet12,morales
Open
TORy1,noiseexit01d,ch...
Open
TORy1,Q617,RedLantern
Open
morales
Open
oilsrv1
Open

洋葱路由应用演示(4/4)

www.ip138.com IP查询(搜索IP地址的地理位置)

您的IP地址是：[173.254.192.38] ARIN

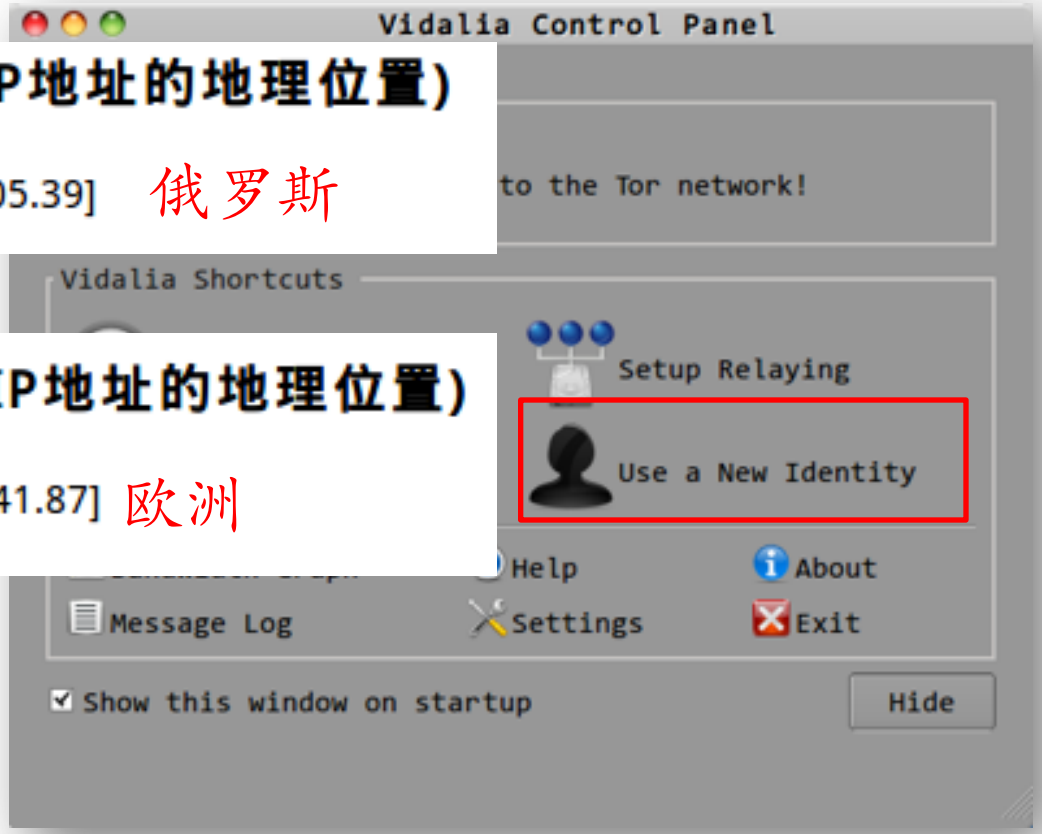
www.ip138.com IP查询(搜索IP地址的地理位置)

您的IP地址是：[89.253.105.39] 俄罗斯

www.ip138.com IP查询(搜索IP地址的地理位置)

您的IP地址是：[84.22.141.87] 欧洲

网络来源标识随你伪造!



联想?

- 匿名通信技术放大了网络安全对抗的复杂性
  - —根据IP地址识别?
    - 不靠谱
  - —根据路由识别?
    - 不靠谱
- 混合应用多种代理技术就可以逃避网络安全审计?
  - —魔高一尺道高一丈
- 网络安全不可抱有侥幸心理

本章内容提要

- 常见代理服务
  - —HTTP代理
  - —虚拟专用网(VPN)
  - —SOCKS代理
- 高级代理服务
- 代理服务的检测

检测需求

- 网络流量计费

  —避免计费误差和损失

- 网络安全审计

  —打击网络攻击源头

- 网络滥用

  —打击网络滥用源头

代理服务的检测手段

- 静态特征

  —协议关键字

- 动态特征

  —流量统计特征

代理服务的检测——静态特征

- 端口扫描
- 协议字段变量特征
  - —网络数据报文
    - 头部字段
    - 负载数据

端口扫描检测方式

- 端口扫描方式主要适用于对代理服务器的检测
- 代理服务器一般最为常用的端口有8080/3218等，可以通过扫描这些端口获得。
- 对于采用非常用端口的代理服务器，端口扫描方式的效率低，准确性也差。

检测手段-变量特征

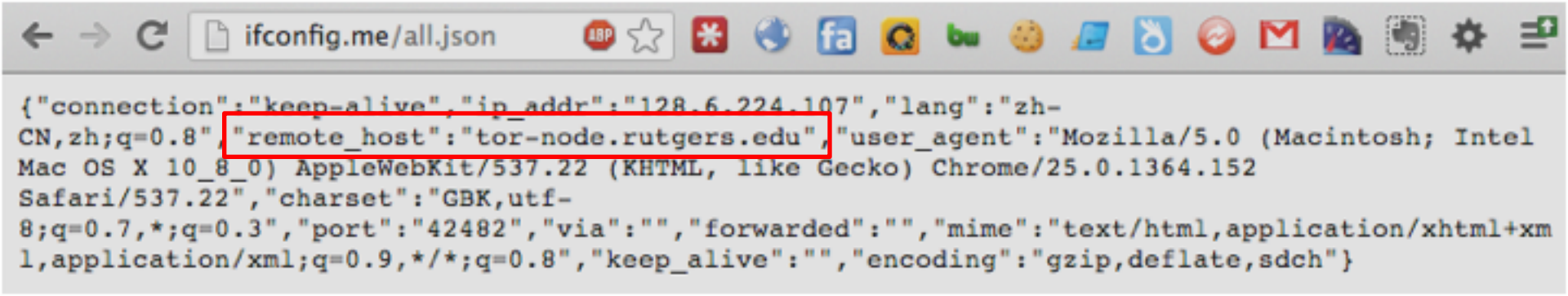
- 常见的变量特征：
  - —VIA
  - —X-FORWARDED-FOR
  - —CACHE-CONTROL
  - —FORWAREDED
  - —PROXY-CONNECTION

代理服务的检测——动态特征

- 协议行为特征
  - —流量形状攻击
    - 通信模式攻击
    - 消息频度攻击
    - 报文计数攻击
  - —交集攻击
  - —重放攻击
  - —刷新攻击
  - —时间攻击

代理服务检测-Demo (1/2)

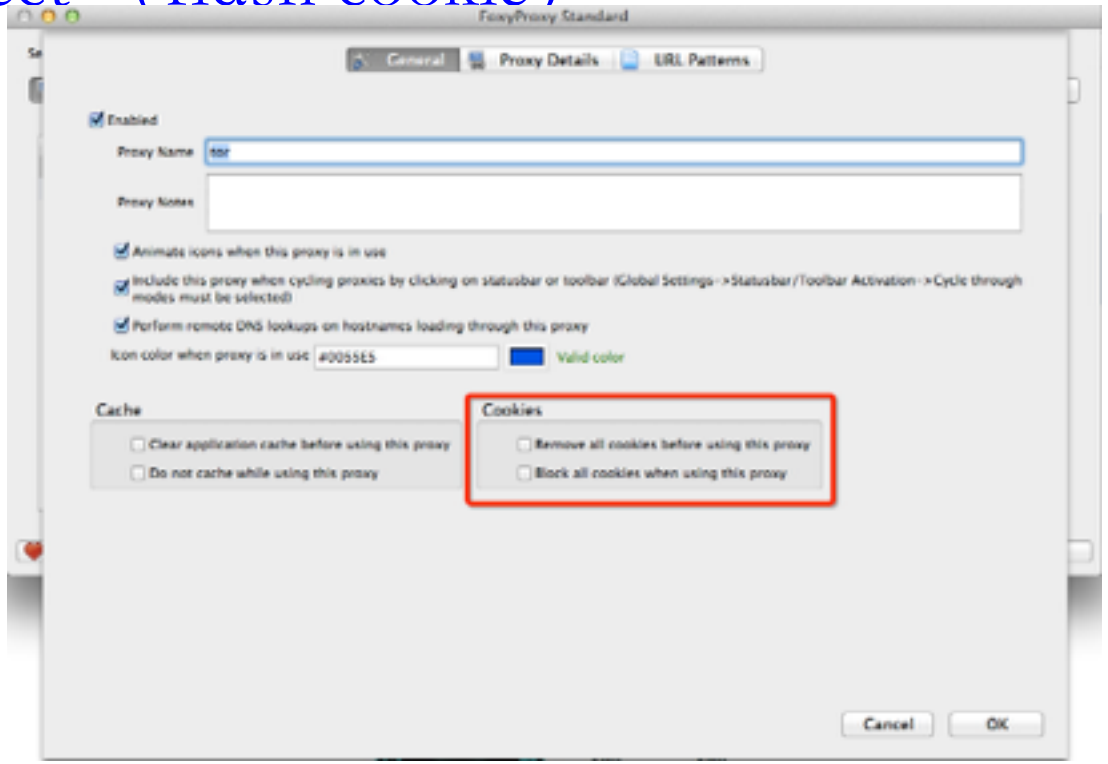
- 设置浏览器使用HTTP代理
- 伪造HTTP请求头
  - —X-Forwarded-For设置单个、多个IP地址
  - —X-Forwarded-For设置任意字符
- 洋葱路由匿名代理服务的检测
  - —利用cookie机制
  - —小心remote_host字段泄漏：你正在使用tor!



代理服务检测-Demo (2/2)

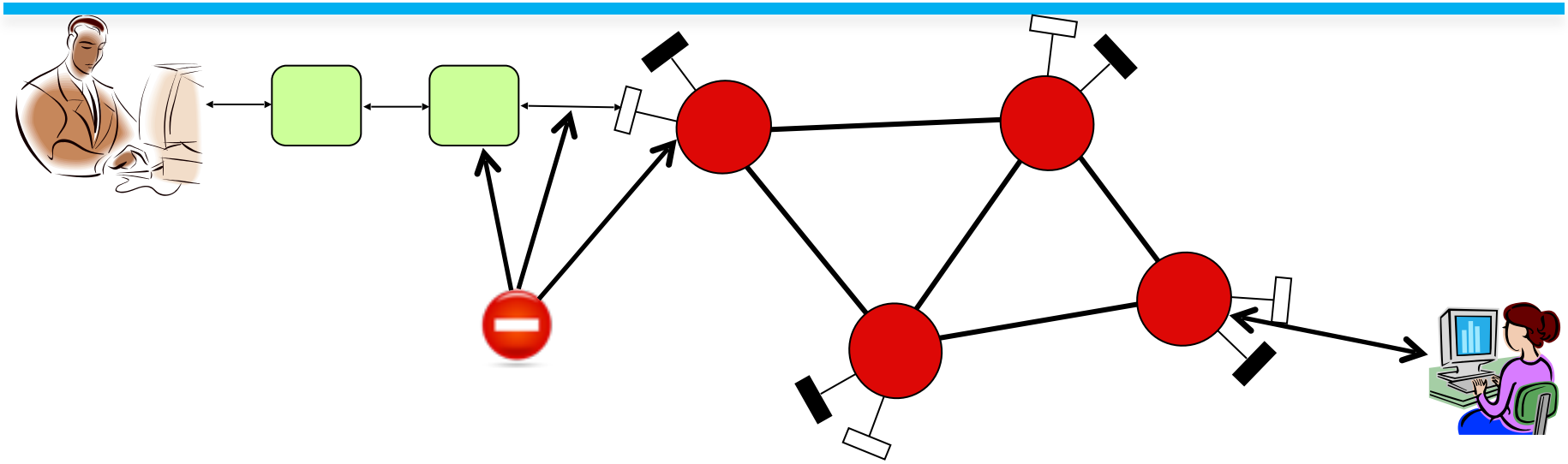
- 小心浏览器的“标识”泄漏你的真实身份
  - —浏览器cookie
  - —Flash Shared Object （flash cookie）
  - —HTML5本地存储

右图：Firefox的foxyproxy扩展配置界面



http://cs.cuc.edu.cn/huangwei/works/index-3.html

关于代理检测的深入思考



- 代理检测方法的效果取决于检测方所拥有的资源多少、权限大小
  - —主机、交换机、路由器、核心网交换机、ISP路由器。。。
  - —主机监控软件、网络嗅探、网络篡改。。。

审查 VS. 反审查

攻击 VS. 防御

对抗!

跟踪 VS. 反跟踪

解密 VS. 加密

实名 VS. 匿名

参考文献

① Proxy server http://en.wikipedia.org/wiki/Proxy_server

② X-Forwarded-For http://en.wikipedia.org/wiki/X-Forwarded-For

③ D. Chaum, Untraceable Electric Mail, Return Address and Digital Pseudonyms, Communication of A.C.M 24.2 (Feb 1981), 84-88

④ M. Reiter and A. Rubin, Crowd: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1(1) June 1998

⑤ Managing HTML5 Offline Storage on Google Chrome https://developers.google.com/chrome/whitepapers/storage

课后思考题

- 代理技术在网络攻防中的意义?
  - —对攻方的意义?
  - —对守方的意义?
- 常规代理技术和高级代理技术的设计思想区别与联系?